Using Windows 2000 with Service Pack 3 in a Managed Environment: Controlling Communication with the Internet

Microsoft Corporation

Published: March 2003

Table of Contents

Introduction

Microsoft® Windows® 2000 operating systems include a variety of technologies that communicate with the Internet to provide an improved user experience. Browser and e-mail technologies are obvious examples, but there are also technologies such as Automatic Updates that help users obtain the latest software and product information, including bug fixes and security patches. These technologies provide many benefits, but they also involve communication with Internet sites, which administrators might want to control.

Control of this communication can be achieved through a variety of options built into individual components, into the operating system as a whole, and into server components designed for managing configurations across your organization. For example, as an administrator you can use Group Policy to control the way some components communicate, or for some components, you can direct all communication to the organization's own internal Web site instead of an external site on the Internet.

This white paper provides information about the communication that flows between components in Windows 2000 Service Pack 3 (SP3) and sites on the Internet, and describes steps to take to limit, control, or prevent that communication in an organization with many users. The white paper is designed to assist you, the administrator, in planning strategies for deploying and maintaining Windows 2000 SP3 in a way that helps provide an appropriate level of security for your organization's networked assets.

This white paper provides guidelines for controlling components in the following operating systems:

- Windows 2000 Professional with SP3.
- Products in the Windows 2000 Server family with SP3. The Windows 2000 Server family includes Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Datacenter Server.

The white paper is organized around individual components found in Windows 2000 SP3, so that you can easily find detailed information for any component you are interested in.

Information about Service Pack 3 for Windows 2000

If you are using Windows 2000, we strongly recommend that you install SP3 or later. Windows 2000 SP3 and all later Windows 2000 service packs contain many valuable improvements, including improvements in application compatibility, operating system reliability, and setup. Also included are necessary improvements to security, such as updates that close potential vulnerabilities. This subsection outlines the following information about Service Pack 3 for Windows 2000:

- A description of the fact that some features in Windows 2000 SP3 work slightly differently from features in Windows 2000 without SP3.
- A description of integrated installation, in which the operating system is installed with the service pack already integrated into it. This contrasts with an installation where Windows 2000 is installed and the service pack is applied afterward.

- Information about certain components, such as Windows Media® Player, for which different versions can be installed even when the operating system version remains Windows 2000 SP3.

Changes to components after SP3 is applied

Although many components described in this white paper are the same with or without SP3, some components operate differently if SP3 has been applied to Windows 2000. For example, if SP3 has been applied, Windows Update includes Automatic Updates, and it therefore operates differently. (The description of Windows Update in this paper includes Automatic Updates.)

Integrated and unattended installation

You can install Windows 2000 and apply the service pack afterward, although there is an additional option. You can apply the service pack directly to the Windows 2000 installation files and complete an integrated installation by using a shared distribution folder on a network. It is also possible to create a CD to complete the installation after you have integrated the files.

If you combine integrated installation (network-based or CD-based) with unattended installation methods, several additional answer-file entries will work (these entries will not work with unattended installation of Windows 2000 alone). These entries affect several components described in this white paper. For more details about integrated and unattended installation and the answer-file entries that work only with an integrated installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."

Important You cannot remove a service pack that you installed with Windows 2000 in an integrated installation.

Component versions

There are some cases where an individual component such as Microsoft Internet Explorer comes in multiple versions, and you can download a newer version after downloading SP3 for Windows 2000. In most of these cases, the component version covered in this white paper is the version originally built into Windows 2000 SP3. There are, however, several exceptions:

- **Internet Explorer and Outlook Express**: The white paper focuses on the versions of these components installed with Windows 2000 SP3, that is, Internet Explorer 5.01 SP3 and Outlook Express 5.50.4807.1700. Pointers are provided, however, to additional information for a newer version of Internet Explorer and Outlook Express, that is, version 6 SP1, which you can easily download after you download SP3 for Windows 2000. We recommend including version 6 SP1 of Internet Explorer and Outlook Express in your deployment. For more information, see the sections of this white paper that describe these components.
- **Windows Media Player**: Windows Media Player 9 Series is the version described in this white paper. As described in the section about Windows Media Player, we recommend that you take one of the following two approaches to Windows Media Player on clients, depending on the intended use of the client:
    - **On a client used for viewing streaming media**: If the client will be used for viewing streaming media (for example, music or videos), we recommend that you upgrade to Windows Media Player 9 Series on that client and on all servers from which you want to control that client. Completing these upgrades makes it easier to control Windows Media

Player at an administrative level, and therefore makes it easier to limit the ways that users can initiate communication with Internet sites through Windows Media Player.

- **On a client not used for viewing streaming media**: If the client will not be used for viewing streaming media, remove the visible entry points to Windows Media Player on that client, and as an additional option, use Group Policy to prevent the user from running the Windows Media Player executable, Wmplayer.exe. These methods help prevent users from starting Windows Media Player and from initiating communication with Internet sites through Windows Media Player.

What this white paper covers and what it does not cover

The subsections that follow describe:

- Types of components covered in this white paper
- Types of components not covered in this white paper
- Security basics that are beyond the scope of this white paper, with listings of some other sources of information about these security basics

Types of components covered in this white paper

This white paper provides:

- Information about components that in the normal course of operation send information to or receive information from one or more sites on the Internet. An example of this type of component is Automatic Updates; if a user chooses to use this component, software updates can be downloaded from a site on the Internet.
- Information about components that routinely display buttons or links that make it easy for a user to initiate communication with one or more sites on the Internet. An example of this type of component is Event Viewer; if a user opens an event in Event Viewer and clicks a link, the user is prompted with a message box that says, "Event Viewer will send the following information across the Internet. Is this OK?" If the user clicks OK, information about the event is sent to a Web site, which replies with any additional information that might be available about that event.
- Brief descriptions of components like Internet Explorer and Internet Information Services (IIS) that are designed to communicate with the Internet. It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running servers that communicate across the Internet, or where users connect to sites on the Internet, download items from the Internet, send and receive e-mail, and perform similar actions. This white paper does, however, provide basic information about how components such as Internet Explorer and Internet Information Services work, and it provides suggestions for other sources of information about balancing your organization's requirements for communication across the Internet with your organization's requirements for protection of networked assets.

Types of components not covered in this white paper

This white paper does not provide:

- Information about managing or working with applications, scripts, utilities, Web interfaces, Microsoft ActiveX® controls, extensible user interfaces, the .NET Framework, and application programming interfaces (APIs). These are either applications, or are layers that support applications, and as such provide extensions that go beyond the operating system itself.

  Windows Installer is not covered in this white paper, although Windows Installer includes some technology that (if you choose) you can use for installing drivers or other software from the Internet. Such Windows Installer packages are not described because they are like a script or utility specifically created for communication across the Internet.

  Note that among the applications not covered in this white paper are Web-based and server-based applications, for example, server-based applications for databases, e-mail, or instant messaging. You must work with your software provider to learn what you can do to mitigate any risks that are part of using particular applications (including Web-based or server-based applications), scripts, utilities, and other software that runs on Windows 2000 SP3.

- Information about components that store local logs that could potentially be sent to someone or could potentially be made available to support personnel. For example, the white paper does not have a section about the Windows Report Tool, with which you can create a diagnostic report that is stored on your computer. Information in such a report or in a log file is similar to any other type of information that can be sent through e-mail or across the Internet in other ways. You must work with your support staff to provide guidelines about the handling of logs and any other similar information you might want to protect.

Security basics that are beyond the scope of this white paper

This white paper is designed to help you, the administrator, plan strategies for deploying and maintaining Windows 2000 SP3 in a way that helps provide an appropriate level of security for your organization's networked assets. The paper does not describe security basics, that is, strategies and risk-management methods that provide a foundation for security across your organization. It is assumed you are actively evaluating and studying these security basics as a standard part of network administration.

Some of the security basics that are a standard part of network administration include:

- Monitoring. This includes using a variety of software tools, including tools to assess which ports are open on servers and clients.
- Virus-protection software.
- The principle of least privilege (for example, not logging on as an administrator if logging on as a user is just as effective).
- The principle of running only the services and software that are necessary, that is, stopping unnecessary services and keeping computers (especially servers) free of unnecessary software.
- Strong passwords, that is, requiring all users and administrators to choose passwords that are not easily deciphered.
- Risk assessment as a basic element in creating and implementing security plans.
- Software deployment and maintenance routines to help ensure that your organization's software is running with the latest security updates and patches.
- Defense-in-depth. In this context, defense-in-depth (also referred to as in-depth defense) means redundancy in security systems, for example, using firewall settings together with Group Policy to control a particular type of communication with the Internet.

Other sources of information about security basics

The following books and Web sites are a few of the many sources of information about the security basics described previously:

- Howard, Michael, et al. *Designing Secure Web-Based Applications for Microsoft Windows 2000*. Redmond, WA: Microsoft Press, 2000.
- Kaufman, C., Perlman, R., and Speciner, M. *Network Security: Private Communication in a Public World*. Upper Saddle River, New Jersey: Prentice-Hall Inc., 2002.
- Howard, Michael, and David LeBlanc. *Writing Secure Code*. Redmond, WA: Microsoft Press, 2002.
- The Prescriptive Architecture Guides on the Microsoft Technet Web site at:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/idc/pag/pag.asp

Device Manager and Hardware Wizards

This section provides information about:

- The benefits of Device Manager
- How Device Manager communicates with sites on the Internet
- How to control Device Manager to limit the flow of information to and from the Internet

Device Manager interacts with the Internet through the hardware wizards by contacting Windows Update when you install or update hardware. For procedures related to disabling Windows Update see the section in this white paper titled "Windows Update and Automatic Updates."

Benefits and purposes of Device Manager

Device Manager provides users and administrators with information about how the hardware on their computers is installed and configured, and how the hardware interacts with the computer's applications. With Device Manager, administrators can update the drivers (or software) for hardware devices, modify hardware settings, and troubleshoot problems.

Note Only administrators or users with administrative credentials can install or update device drivers.

Overview: Using Device Manager in a managed environment

Administrators can access Device Manager on a computer running Microsoft Windows 2000 Service Pack 3 (SP3) through Administrative Tools\Computer Management. Users can access Device Manager through the Control Panel\System\Hardware tab to view information about the hardware installed on their computers, but they must have administrative credentials to modify or update hardware.

Administrators or users with administrative credentials will typically use Device Manager to check the status of hardware and to update device drivers. Administrators who have a thorough understanding of computer hardware might also use Device Manager's diagnostic features to resolve device conflicts and change resource settings.

Device Manager can communicate with the Internet when an administrator uses it to update a driver. To update a driver you select the **Properties** page of a hardware device and click the **Driver** tab. When you select **Update Driver** the Upgrade Device Driver Wizard appears. In the wizard the administrator can choose to have Windows Update as a search location for driver files.

Note Windows Update is not automatically contacted for driver updates. The administrator has to select Windows Update as a search location.

Device Manager works in conjunction with Windows Update to deliver updated drivers for installed hardware devices. As an IT administrator in a highly managed environment you might

want to block certain administrators from downloading drivers through Device Manager. You can do this by configuring Group Policy to disable Windows Update. If you disable Windows Update then Device Manager cannot communicate with the Internet. The following subsection provides details about how Device Manager interacts with the Internet.

How Device Manager communicates with sites on the Internet

The way Device Manager communicates with the Internet is based on its interaction with Windows Update through the Upgrade Device Driver Wizard; therefore much of the information in this subsection is the same as for Windows Update. Additional details are described as follows:

- **Specific information sent or received**: See the section "Windows Update and Automatic Updates" in this white paper.
- **Default and recommended settings**: Device Manager is enabled by default. See the subsection "Controlling Device Manger to limit the flow of information to and from the Internet" for recommended settings.
- **Triggers**: Through Device Manager an administrator starts the Upgrade Device Driver Wizard, or adds new hardware to a computer.
- **User notification**: See "Windows Update and Automatic Updates."
- **Logging**: Errors that result from problems installing hardware devices without drivers are logged to the event log.
- **Encryption, access, privacy policy, transmission protocol, and port**: See "Windows Update and Automatic Updates."
- **Ability to disable**: You cannot disable Device Manager directly. You can, however, prevent interaction with the Internet through Device Manager by disabling Windows Update.

Controlling Device Manager to limit the flow of information to and from the Internet

You can prevent the Internet from being accessed through Device Manager by disabling Windows Update using the following Group Policy setting: **Remove access to use all Windows Update features**. In the Group Policy Object Editor, this policy setting is located in User Configuration\Administrative Templates\Windows Components\Windows Update. (To find more information about the Group Policy Object Editor, see Appendix B, "Resources for Learning About Group Policy.")

When you disable access to Windows Update using Group Policy, the policy setting also removes Windows Update as a search location when a user or administrator is updating a driver through Device Manager. Users will still be able to use Device Manager to view information about their hardware devices. For administrators to be able to update drivers there is the option for manually downloading driver updates from the Windows Update Catalog, whereby they can be distributed on your managed network as needed.

For more information about the Windows Update Catalog, see the Windows Update Web site at:

windowsupdate.microsoft.com/

See the section "Windows Update and Automatic Updates" in this white paper for the procedure to disable Windows Update using Group Policy.

Event Viewer

This section provides information about:

- The benefits of Event Viewer
- How Event Viewer communicates with sites on the Internet
- How to control Event Viewer to prevent the flow of information to and from the Internet

Benefits and purposes of Event Viewer

Administrators can use Event Viewer to view and manage event logs. Event logs contain information about hardware and software problems and about security events on your computer. A computer running Microsoft Windows 2000 Service Pack 3 (SP3) records events in three kinds of logs: application, system, and security. While Event Viewer is primarily a tool for administrators to manage event logs, users can also view application and system logs on their computer. Only administrators can gain access to security logs.

Overview: Using Event Viewer in a managed environment

Users can access event logs for their own computer through Control Panel\Administrative Tools\Event Viewer. The user can obtain detailed information about a particular event by either double-clicking the event, or by selecting the event and clicking **Properties** on the Action menu. The dialog box gives a description of the event, which might also contain a link to a Web site.

Links can either be to Microsoft servers, or to servers managed by the software vendor for the component that generated the event. In Windows 2000, some events that originate from Microsoft products, such as Microsoft Exchange, have a description containing a URL that the user can click for more information ("For additional information specific to this message please visit the Microsoft Online Support site located at http://www.microsoft.com/contentredirect.asp").

When users click the link, they are asked to confirm that the information presented to them can be sent over the Internet. If the user clicks Yes, the information listed will be sent to the Web site named in the link. The parameters in the original URL will be replaced by a standard list of parameters whose contents are detailed in the confirmation dialog box. This list is provided in the next subsection under "Specific information sent or received."

How Event Viewer communicates with sites on the Internet

In order to access the relevant Help information provided by the link in the Event Properties dialog box, the user sends the information listed about the event. The collected data is confined to what is needed to retrieve more information about the event from the Microsoft Knowledge Base. User names and e-mail addresses, names of files unrelated to the logged event, computer addresses, and any other forms of personally identifiable information are not collected.

The exchange of information that takes place over the Internet is described as follows:

- **Specific information sent or received**: Information about the event sent over the Internet consists of the URL in the link (minus the parameters after the "?") and the standard parameters. The standard parameters are all listed in the confirmation dialog box. They include the following:
  - Company name (name of the software vendor for this component, not your organization; for example, Microsoft Corporation)
  - Event ID (for example, 105)
  - File version (for example, 5.0.2195.5995)
  - Product name and version (for example, Internet Information Services, 5.0.2195.5995)
  - Source (for example, W3SVC)

  The information the user receives is from the Web site named in the link.
- **Default settings**: Access to Event Viewer is enabled by default.
- **Triggers**: The user chooses to send information about the event over the Internet in order to obtain more information about the event.
- **User notification**: When a user clicks the link, a dialog box listing the information that will be sent is provided.
- **Logging**: This is a feature of Event Viewer.
- **Encryption**: The information may or may not be encrypted, depending on whether it is an HTTP or HTTPS link.
- **Access**: No information is stored.
- **Transmission protocol and port**: Communication occurs over the standard port for the protocol in the URL, either HTTP or HTTPS.

Controlling Event Viewer to prevent the flow of information to and from the Internet

In Windows 2000 you cannot directly disable the links to Web sites provided in some event descriptions. To control the ability of users to make connections to the Internet through Event Viewer, use one or more of the following methods:

- If appropriate, instruct users about this or any other options that you want them to avoid in Event Viewer.
- Using a firewall, proxy server, or both, limit the sites that users can connect to on the Internet.
- Set up your networks so that some computers do not have connections to the Internet, if this conforms to your organization’s goals and security requirements.

HyperTerminal

This section provides information about:

- The benefits of HyperTerminal
- How HyperTerminal communicates with sites on the Internet
- How to control HyperTerminal to prevent the flow of information to and from the Internet

Benefits and purposes of HyperTerminal

HyperTerminal is a program that you can use to connect to other computers, Telnet sites, bulletin board systems (BBSs), online services, and host computers. HyperTerminal connections are made using a modem, a null modem cable (used to emulate modern communication), or an Ethernet connection.

HyperTerminal has capabilities beyond making connections to other computers. It can, for example, transfer large files from a computer onto your portable computer using a serial port rather than requiring you to set up your portable computer on a network. It can also help debug source code from a remote terminal. It can also communicate with many older, character-based computers.

HyperTerminal records the messages passed to and from the computer or service on the other end of your connection. It can therefore serve as a valuable troubleshooting tool when setting up and using your modem. To make sure that your modem is connected properly or to view your modem's settings, you can send commands through HyperTerminal and check the results. HyperTerminal also has scroll functionality that enables you to view received text that has scrolled off the screen.

Note HyperTerminal is designed to be an easy-to-use tool yet it is not meant to replace other full-featured tools. You can use HyperTerminal as described in this subsection, but you should not attempt to use HyperTerminal for more complex communication. For more information about what HyperTerminal does and does not support, see the list of frequently asked questions on the Hilgraeve Web site at:

www.hilgraeve.com/support/faq/index.html

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Overview: Using HyperTerminal in a managed environment

In a managed environment, providing access to local and remote connection points through the use of HyperTerminal may pose security risks. You can therefore remove HyperTerminal from Microsoft Windows 2000 Service Pack 3 (SP3) components during installation as described later in this section. Following are a few security issues to consider when deciding how to configure HyperTerminal for your organization:

- **Viruses**: Incoming files might contain viruses or malicious programs that could compromise or destroy data on your computer. To reduce this risk, use virus-scanning software and ensure that incoming files are from a reliable and trusted source.
- **ID and password**: HyperTerminal cannot automatically provide your login ID and password when you make a connection. If you provide a password when using HyperTerminal for a Telnet session, be aware that this password will be sent to the remote computer using plaintext (as with all Telnet connections).
- **Automatic download**: The automatic download feature of the Zmodem protocol can pose a security risk by allowing remote users to send files to your computer without your explicit permission. To avoid this risk, you should select a protocol other than Zmodem in the Receive File dialog box or you should clear the **Allow remote host-initiated file transfers** check box on the Settings tab of Connection Properties.

Complete information about concepts and procedures associated with using or configuring HyperTerminal is beyond the scope of this white paper. For more information, look up "HyperTerminal" in the Windows Help index.

How HyperTerminal communicates with sites on the Internet

The exchange of information that takes place during the HyperTerminal connection is described as follows:

- **Specific information sent or received**: When using HyperTerminal for Telnet connectivity, the user ID and password are sent in plaintext format. If files are being transmitted, only the protocol, terminal emulation data, and file-specific binaries are sent. The computer running HyperTerminal is identified by its IP address when the connection type is TCP/IP. The computer is not uniquely identified when the connection type is not TCP/IP.
- **Default settings**: HyperTerminal is installed by default on computers running Windows 2000 SP3 and Windows XP Professional SP1. To remove or uninstall HyperTerminal, see "Controlling HyperTerminal to prevent the flow of information to and from the Internet," later in this section.
- **Triggers**: When HyperTerminal is set to automatically answer incoming connections, a file transfer can be initiated if the Zmodem transfer protocol is used. Otherwise, communication through HyperTerminal is only triggered when the user deliberately initiates it.
- **User notification**: After a user starts a HyperTerminal connection session, the status of the connection that is currently open within HyperTerminal is displayed in the HyperTerminal title bar. The status of the file and text transfer is displayed in the HyperTerminal window during the transfer process. HyperTerminal does not display connection or transfer status information when the automatic download feature of the Zmodem protocol is used. For more information about the HyperTerminal automatic download feature, see "Overview: Using HyperTerminal in a managed environment," earlier in this section.
- **Encryption:** Information sent or received by HyperTerminal is not encrypted.
- **Transmission protocol and port**: The protocols used are Kermit, Xmodem, 1K Xmodem, Ymodem, Ymodem-G, and Zmodem transmissions protocols on port 23.
- **Ability to disable**: You can remove the visible entry points for HyperTerminal, or configure the answer file for unattended installation not to install HyperTerminal during the deployment process. To remove or uninstall HyperTerminal, see "Controlling HyperTerminal to prevent the flow of information to and from the Internet," later in this section.

Controlling HyperTerminal to prevent the flow of information to and from the Internet

HyperTerminal is installed by default on all computers running Windows 2000 SP3. You can prevent the use of HyperTerminal by disabling it through unattended installation during deployment, or by removing the visible entry points for HyperTerminal after installing Windows 2000 SP3.

The following procedures describe:

- How to specify the HyperTerminal installation options in an answer file during an unattended installation of Windows 2000 SP3.
- How to use the Add/Remove Programs utility in Control Panel to remove the visible entry points to HyperTerminal after the deployment of Windows 2000 SP3.

To remove visible entry points to HyperTerminal during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, include the following entry:

   hyperterm = Off

To remove visible entry points to HyperTerminal on an individual computer running Windows 2000 SP3

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Double-click **Accessories and Utilities,** and then double-click **Communications**.
5. Make sure the check box for the HyperTerminal component is cleared.
6. Follow the instructions to complete the Windows Components Wizard.

Note You must have administrative credentials to complete this procedure.

Related links

- For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
- For more information about what HyperTerminal does and does not support, see the HyperTerminal list of frequently asked questions on the Hilgraeve Web site at:

  www.hilgraeve.com/support/faq/index.html

Using online resources. The Microsoft Web site contains support information, including the latest downloads and Knowledge Base articles written by support professionals at Microsoft:

- You can search frequently asked questions (FAQs) by product, browse the product support newsgroups, and contact Microsoft Support at the following Web site. You can also search the Microsoft Knowledge Base of technical support information and self-help tools for Microsoft products at this site:

  support.microsoft.com/

- You can search for troubleshooting information, service packs, patches, and downloads for your system on the TechNet Web site at:

  www.microsoft.com/technet/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Internet Explorer 5.01 SP3

This section provides information about:

- The benefits of Microsoft Internet Explorer 5.01 Service Pack 3 (SP3), which is the version of Internet Explorer that is installed with Windows 2000 Service Pack 3 (SP3).

  At the end of this section of the white paper, there are links to information about Internet Explorer 6 SP1, which is readily available for downloading. If you are deploying Windows 2000 SP3 across an organization, we recommend that you consider including Internet Explorer 6 SP1 in your deployment instead of Internet Explorer 5.01 SP3, because Internet Explorer 6 SP1 offers additional security-related options and settings. If you include Internet Explorer 6 SP1 in your deployment, the required order for downloading is Windows 2000 SP3 first and Internet Explorer 6 SP1 second (restarting after each download).

- Steps for planning and deploying configurations for Internet Explorer 5.01 SP3 in a way that balances your users' requirements for Internet access with your organization's requirements for protection of networked assets.

- Examples of the security-related features offered in Internet Explorer 5.01 SP3.

- Resources for learning about topics related to security in Internet Explorer 5.01 SP3. This includes resources that help you learn about:

  - Security settings in Internet Explorer 5.01 SP3.

  - Reducing the risks inherent in Web-based applications and scripts.

  - Methods for deploying specific configurations of Internet Explorer 5.01 SP3 across your organization using Group Policy.

- Information about removing all visible entry points to Internet Explorer in Microsoft Windows 2000 Professional with Service Pack 3 (SP3), for situations where you do not want users to have access to Internet Explorer, or where you want users to use another Web browser exclusively. There are several ways to do this:

  - During unattended installation.

  - Through Add/Remove Programs in Control Panel.

  - With **Set Program Access and Defaults**, through which the administrator of a computer running Windows 2000 Professional with SP3 can specify which Web browser is shown on the Start menu, desktop, and other locations.

Note
This section of the white paper describes Internet Explorer 5.01 SP3 in general, but it does not describe Outlook Express (the e-mail component in Internet Explorer) or the Internet Connection Wizard. This section also does not describe Internet Information Services (IIS), the component that supports the creation of Web sites on a server. For information about these components, see the respective sections of this white paper.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization where users connect to Web sites, run software from the Internet, download items from the Internet, and perform similar actions. This section, however, provides overview information as well as suggestions for other sources of information about how to

balance users' requirements for Internet access with your organization's requirements for protection of networked assets.

For more information about Internet Explorer, see the following resources:

- Help for Internet Explorer (with Internet Explorer open, click the **Help** menu and select an appropriate option)
- The Internet Explorer page on the Microsoft Web site at:

  www.microsoft.com/windows/ie/
- The resource page for previous versions of Internet Explorer at:

  www.microsoft.com/windows/ieak/previous/
- The Resource Kit for Internet Explorer. To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

  www.microsoft.com/reskit/

Benefits and purposes of Internet Explorer 5.01 SP3

Internet Explorer 5.01 SP3 is designed to make it easy to browse and interact with sites on an intranet or on the Internet. It differs from many of the other components described in this white paper in that its main function is to communicate with sites on the Internet or an intranet (which contrasts with components that communicate with the Internet in the process of supporting some other activity).

Internet Explorer 5.01 SP3 is also designed to be configurable by an administrator (or in an unmanaged environment, a user), with security settings that can help protect your organization's networked assets while at the same time providing users with access to useful information and tools.

With an understanding of the settings and options available in Internet Explorer 5.01 SP3, you can choose the settings appropriate to your organization's requirements, and create a plan for one or more standard Internet Explorer configurations. After planning your standard configurations, you can use deployment tools to deploy and maintain them. The subsections that follow provide more information about these steps.

Steps for planning and deploying configurations for Internet Explorer 5.01 SP3

This subsection outlines a list of steps that can help you deploy Internet Explorer 5.01 SP3 in a way that provides users with Internet access, while at the same time helping to provide your organization's networked assets with an appropriate level of protection from the risks inherent in the Internet. (If you prefer to remove all visible entry points to Internet Explorer when you perform unattended installation, see "Excluding Internet Explorer 5.01 SP3 from the desktop," later in this section.)

A recommended set of steps is:

- Assess the other elements in your security plan that will work together with Internet Explorer 5.01 SP3 to help provide users with access to the Internet while providing

an appropriate degree of protection for your organization's networked assets. These elements include:

- Your proxy server.
- Your firewall.
- Your basic security measures, as described in the introduction to this white paper. These security measures include using virus-protection software and setting requirements for strong passwords.

It is beyond the scope of this white paper to provide detailed recommendations for these security elements. For more information about security, see the references listed in the introduction, as well as the documentation for your proxy server, firewall, virus-protection software, and other software you use to protect networked assets.

- Learn about the security-related features offered in Internet Explorer 5.01 SP3, some of which are described in "Examples of the security-related features offered in Internet Explorer 5.01 SP3," later in this section. Using information about these features, identify the ones of most value for your business and security requirements.
- Learn how to configure security settings in Internet Explorer 5.01 SP3, as described in "Learning about security settings in Internet Explorer 5.01 SP3," later in this section.
- Learn about ways to reduce the risks inherent in code that can be run through a browser, as described in "Learning about reducing the risks inherent in Web-based applications and scripts," later in this section.
- After gathering information about the previous three items (security-related features, security settings, risks inherent in code), plan one or more standard Internet Explorer configurations for the desktops in your organization.
- Learn about using Group Policy to control the configuration of Internet Explorer 5.01 SP3 on desktops across your organization, as described in "Learning about Group Policy objects (GPOs) that control configuration settings for Internet Explorer 5.01 SP3," later in this section.

  Using the information about Group Policy, create a plan for deploying and maintaining your standard Internet Explorer configurations.

Excluding Internet Explorer 5.01 SP3 from the desktop

For information about removing visible entry points to Internet Explorer in Windows 2000 Professional with SP3, see "Procedures for removing visible entry points to Internet Explorer in Windows 2000 Professional with SP3" later in this section.

Examples of the security-related features offered in Internet Explorer 5.01 SP3

This subsection describes enhancements in some of the security-related features in Internet Explorer 5.01 SP3. These features include:

- Security settings that specify how Internet Explorer 5.01 SP3 handles such higher-risk items as ActiveX controls, downloads, and scripts. These settings can be customized as needed, or they can be set to these predefined levels: high, medium, medium-low, or low. You can specify different settings for a number of zones, the most basic being the four preconfigured zones:

- Local intranet zone: Contains addresses inside your proxy server.
- Trusted sites: Includes sites you designate as "trusted."
- Restricted sites: Includes sites you designate as "restricted."
- Internet zone: Includes everything that is not in another zone and is not on the local computer.

You can also specify different settings for the following zone:

- Customized zones: These are added programmatically using the URL security zones application programming interface (API). For more information about this API, see the Microsoft Developer Network Web site at:

  msdn.microsoft.com/

- Improvements in Service Pack 3 that increase the overall security and reliability of Internet Explorer 5.01.

For more information about features available in Internet Explorer, see the information in the next subsection, as well as the Internet Explorer page on the Microsoft Web site at:

www.microsoft.com/windows/ie/

Resources for learning about topics related to security in Internet Explorer 5.01 SP3

This subsection lists resources that can help you learn about the following topics related to security in Internet Explorer 5.01 SP3:

- Security settings available in Internet Explorer 5.01 SP3
- Methods for reducing the risks inherent in Web-based applications and scripts
- Ways to use Group Policy objects (GPOs) that control configuration settings for Internet Explorer 5.01 SP3

In addition, for information about unattended installation, see the resources listed in Appendix A, "Resources for Learning About Automated Installation and Deployment."

Learning about security settings in Internet Explorer 5.01 SP3

An important source of detailed information about security settings in Internet Explorer 5.01 SP3 is the Microsoft Internet Explorer 5.0 Resource Kit. To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

www.microsoft.com/reskit/

The Microsoft Internet Explorer 5.0 Resource Kit consists of a number of chapters that cover topics such as the following:

- Security zones
- Deployment planning

- Customizing (including system policies and restrictions, described in an appendix in the Internet Explorer 5.0 Resource Kit)
- Maintenance and support, including information about keeping software updated

Learning about reducing the risks inherent in Web-based applications and scripts

In a network-based and Internet-based environment, code can take a variety of forms including scripts within documents, scripts within e-mail, or applications or other code objects running within Web pages. This code can move across the Internet and is sometimes referred to as "mobile code." Configuration settings provide ways for you to control the way Internet Explorer 5.01 SP3 responds when a user tries to run mobile code. Two examples of the ways you can customize the Internet Explorer configuration deployed in your organization are as follows:

- You can control the code (in ActiveX controls or in scripts, for instance) that users can run. You can do this by customizing Authenticode settings, which can, for example, prevent users from running any unsigned code or enable them to only run code signed by specific authors.
- If you want to permit the use of ActiveX controls, but do not want users to download code directly from the Internet, you can specify that when Internet Explorer 5.01 SP3 looks for a requested executable, it goes to your own internal Web site instead of the Internet. For more information, see the white paper titled "Managing Mobile Code with Microsoft Technologies" at the end of this list, and search for "CodeBase."

You can use the following sources to learn more about reducing the risks inherent in Web-based applications and scripts:

- To understand more about how a particular Microsoft programming or scripting language works, see the Microsoft Developer Network Web site at:

  msdn.microsoft.com/

- To learn about approaches to reducing the risks presented by mobile code, see "Managing Mobile Code with Microsoft Technologies," a white paper on the Technet Web site at:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/mblcode.asp

Learning about Group Policy objects (GPOs) that control configuration settings for Internet Explorer 5.01 SP3

You can control configuration settings for Internet Explorer 5.01 SP3 by using Group Policy objects (GPOs) on servers running Windows 2000. For sources of information about Group Policy, see the appropriate appendices in this white paper.

To learn about specific Group Policy settings that can be applied to computers running Windows 2000, see the Windows 2000 Group Policy Reference at:

www.microsoft.com/windows2000/techinfo/reskit/en-us/gp/default.asp?frame=true

On this Web site, to view one section especially relevant to Internet Explorer, click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Internet Explorer**.

Procedures for removing visible entry points to Internet Explorer in Windows 2000 Professional with SP3

This subsection provides information about removing all visible entry points to Internet Explorer in Windows 2000 Professional with SP3, for situations where you do not want users to have access to Internet Explorer, or where you want users to use another Web browser exclusively. The procedures explain how to do the following:

- Remove visible entry points with **Set Program Access and Defaults**, through which the administrator of a computer running Windows 2000 Professional with SP3 can specify which Web browser is shown on the Start menu, desktop, and other locations.
- Remove visible entry points through Add/Remove Programs in Control Panel.
- Remove visible entry points during unattended installation.

To specify which Web browser is shown on the Start menu, desktop, and other locations on a computer running Windows 2000 Professional with SP3

To perform the following procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.

> **Note** **Set Program Access and Defaults** appears on Windows 2000 Professional with SP3 only. It does not appear on Windows 2000 Server with SP3, Windows 2000 Advanced Server with SP3, or Windows 2000 Datacenter with SP3.

1. Click **Start** and then click **Set Program Access and Defaults**.
2. Select the default Web browser from the options available.

> **Note** If your program does not appear by name, close the **Set Program Access and Defaults** interface and configure your Web browser as the default program. Then open **Set Program Access and Defaults** and click **Use my current Web browser**. For information about how to configure a program to be the default, contact the vendor of that program. Also, for information about the coding that enables a Web browser to be configured as the default, see the Microsoft Developer Network Web site at:
>
> msdn.microsoft.com/library/en-us/shellcc/platform/shell/programmersguide/shell_adv/registeringapps.asp

3. Select the **Show this program** check box.

For more information about **Set Program Access and Defaults**, see the Microsoft Product Support Services Web site at:

support.microsoft.com/default.aspx?scid=kb%3ben-us%3b327931

To remove visible entry points to Internet Explorer on an individual computer running Windows 2000 Professional with SP3

To perform the following procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is

joined to a domain, members of the Domain Admins group might be able to perform this procedure.

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Scroll down the list of components to Internet Explorer, and make sure the check box for that component is cleared.
5. Follow the instructions to complete the Windows Components Wizard.

To remove visible entry points to Internet Explorer during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, include the following entry:

   IEAccess = Off

   Note You can use IEAccess in an answer file only if you are using the integrated installation method for SP3, which enables you to simultaneously install Windows 2000 and the service pack. If you plan to install Windows 2000 by itself and then later apply SP3, you cannot use IEAccess in an answer file. For more information about the integrated installation methods for SP3, see the Service Pack 3 Installation and Deployment Guide at the following Web site:

   www.microsoft.com/windows2000/downloads/servicepacks/sp3/spdeploy.htm

Related links: Information about Internet Explorer 6 SP1

Internet Explorer 6 SP1 is readily available for downloading. If you are deploying Windows 2000 SP3 across an organization, we recommend that you consider including Internet Explorer 6 SP1 in your deployment instead of Internet Explorer 5.01 SP3, because Internet Explorer 6 SP1 offers additional security-related options and settings. If you include Internet Explorer 6 SP1 in your deployment, the required order for downloading is Windows 2000 SP3 first and Internet Explorer 6 SP1 second (restarting after each download).

The following list provides sources of information about Internet Explorer 6 SP1:

- The Internet Explorer Web site at:

  www.microsoft.com/windows/ie/

- The Internet Explorer section in the white paper titled "Using Windows XP Professional with Service Pack 1 in a Managed Environment." This paper can be found on the Technet Web site at:

  www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

- Help for Internet Explorer: after downloading Internet Explorer, start it, click the **Help** menu, and then select an appropriate option.

- The Resource Kit for Internet Explorer. To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

  www.microsoft.com/reskit/

Internet Information Services

This section provides information about:

- The benefits of Internet Information Services (IIS) in Microsoft Windows 2000 Service Pack 3 (SP3).
- For servers from which you want to offer content on an intranet or the Internet, descriptions of some of the security-related features offered in IIS 5.0, and links to more information about security and IIS 5.0.
- For servers from which you do not want to offer content on an intranet or the Internet, information about excluding or removing IIS from a server.
- For users' computers in your organization, steps to take to keep users from installing IIS on Windows 2000 Professional.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running servers that communicate across the Internet. This section, however, provides overview information as well as suggestions for other sources of information about balancing your organization's requirements for communication across the Internet with your organization's requirements for protection of networked assets.

Benefits and purposes of IIS

IIS 5.0 is one of the optional components in Windows 2000 SP3. IIS is a component that provides an easy way to publish information on the Internet or an intranet. In a managed environment, IIS is usually installed on selected servers only. IIS includes innovative security features and a broad range of administrative features for managing Web sites. By using programmatic features like Active Server Pages (ASP), you can more easily create and deploy scalable, flexible Web applications.

The installation defaults for IIS in Windows 2000 products are as follows:

- IIS is not installed by default with Windows 2000 Professional with SP3.

  It can be added by using Add/Remove Programs in Control Panel.

- IIS is installed by default with products in the Windows 2000 Server family.

  It can be excluded from the installation by clearing a check box in the components list during setup, or by including specific entries in an answer file during unattended setup. IIS can also be removed after setup by using Add/Remove Programs in Control Panel. For more information, see "Excluding or removing IIS from a server running Windows 2000" later in this section.

IIS in Windows 2000 Professional can, by default, service only 10 simultaneous client connections, with one Web site only, and it does not use all the features of the server versions. IIS 5.0 in Windows 2000 Professional (and in products in the Windows 2000 Server family) includes the Microsoft Management Console (MMC) snap-in for managing IIS.

For more information about IIS features, see the following Web sites:

- The IIS 5.0 page (part of the Windows 2000 Server family evaluation pages) at:

www.microsoft.com/windows2000/server/evaluation/features/web.asp

Some of the features described on the preceding Web page are listed in "Examples of the security-related features offered in IIS 5.0," later in this section.

- The IIS security page (part of Technet) at:

  www.microsoft.com/technet/security/prodtech/windows/iis/default.asp

Examples of the security-related features offered in IIS 5.0

IIS 5.0 includes a variety of improvements related to security, including additions to the options available for:

- Authentication
- Certificates
- Encryption
- Auditing
- Other features, including new wizards for simplifying the configuration of access permissions and of certificates

Because authentication is an important part of security for a Web server, the following list provides information about some of the standards-based authentication options available in IIS 5.0:

- **Kerberos V5 protocol**: Web services for the Windows 2000 Server family are fully integrated with the Kerberos security infrastructure. The Kerberos V5 authentication protocol, which provides fast, single logon to servers running Windows 2000, replaces NTLM as the primary security protocol for access to resources within or across Windows 2000 domains.
- **Digest authentication**: Digest authentication is the latest authentication standard of the World Wide Web Consortium (W3C), the organization that sets standards for the Web and HTML.
- **Server-Gated Cryptography**: Server-Gated Cryptography (SGC) is a technology that was previously used, most often by financial institutions, to ensure that all clients, regardless of browser version or other software version, could communicate with the server using 128-bit encryption. Because almost all browser versions in current use support 128-bit encryption, SGC is no longer in common use.
- **Fortezza**: Fortezza is a data protection standard that is widely used by the U.S. government.

In addition, there are a number of articles and tools available to help you maintain awareness and control of the communication to and from Web sites created with IIS 5.0.

For more information about creating Web sites with IIS 5.0 and maintaining appropriate levels of awareness and control over the communication to and from those sites, see the following sources:

- The IIS 5.0 page (part of the Windows 2000 Server family evaluation pages) at:

  www.microsoft.com/windows2000/server/evaluation/features/web.asp

- The IIS security page (part of Technet) at:

  www.microsoft.com/technet/security/prodtech/windows/iis/default.asp

- IIS Help, which you can see after you install IIS by typing the following in your browser Address bar:

  http://localhost/IISHelp/

- The "Internet Information Services Security Overview" chapter on the Microsoft Press Web site at:

  www.microsoft.com/mspress/books/sampchap/4293.asp

- The page for the IIS Lockdown Tool, which can help increase security on a server running IIS, on the TechNet Web site at:

  www.microsoft.com/technet/security/tools/tools/locktool.asp

- The page for the Urlscan Security Tool, which can help increase security on a server running IIS, on the TechNet Web site at:

  www.microsoft.com/technet/security/tools/tools/urlscan.asp

Excluding or removing IIS from a server running Windows 2000

If you have servers that are not Web servers, we recommend that you exclude or remove IIS from those servers. There are several ways to do this:

- One way of excluding or removing the IIS component is to clear the check box for the IIS component in the Windows components list, during or after setup. For more information, see "To include or exclude IIS during Windows 2000 setup" or "To view or change the IIS components currently installed on a computer running Windows 2000" later in this section.

- Another way of excluding or removing the IIS component is by using standard methods for unattended installation or remote installation. If you are using an answer file, the following table shows the IIS entries that apply to the Windows 2000 Server family. All the entries in the table belong in the [Components] section of the answer file.

The following table shows the answer file entries associated with IIS in the Windows 2000 Server family as well as the corresponding registry keys. Do not change the registry keys. They are shown for use in a script that could check whether a particular component is installed on a particular computer. A registry key value of 0x00000000 means the component is not installed, and a value of 0x00000001 means the component is installed.

Answer file entries and registry keys associated with IIS subcomponents for the Windows 2000 Server family

IIS subcomponent	Answer file entry (in the [Components] section)	Registry key (for use in a script that checks whether a component is installed): 0x00000000 means it is not installed; 0x00000001 means it is installed
IIS common files	iis_common = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_common
IIS documentation	iis_doc = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_doc
File Transfer Protocol (FTP) service	iis_ftp = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_ftp
HTML-based administration tools for IIS	iis_htmla = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_htmla
IIS MMC snap-in	iis_inetmgr = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_inetmgr
Network News Transfer Protocol (NNTP) service	iis_nntp = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_nntp
Documentation for the Network News Transfer Protocol (NNTP) service	iis_nntp_docs = Off	No key available
Simple Mail Transfer Protocol (SMTP) service	iis_smtp = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_smtp
Documentation for the Simple Mail Transfer Protocol (SMTP) service	iis_smtp_docs = Off	No key available
World Wide Web (WWW) service	iis_www = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_www
FrontPage server extensions	fp_extensions = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\fp_extensions

Excluding or removing IIS from a client running Windows 2000 Professional

To prevent the flow of information through IIS on clients running Windows 2000 Professional with SP3, remove or exclude this component from installation on those clients. There are several ways to do this:

- One way of excluding or removing the IIS component is to ensure that the check box is cleared for the IIS component in the Windows components list, during or after setup. For more information, see "To include or exclude IIS during Windows 2000 setup" or "To view or change the IIS components currently installed on a computer running Windows 2000" later in this section.
- Another way of excluding or removing the IIS component is by using standard methods for unattended installation or remote installation. If you are using an answer file, the following table shows the IIS entries that apply to Windows 2000 Professional. All the entries in the table belong in the [Components] section of the answer file.

  Note By default, the components listed in the table are not installed with Windows 2000 Professional.

The following table shows the answer file entries associated with IIS in Windows 2000 Professional as well as the corresponding registry keys. Do not change the registry keys. They are shown for use in a script that could check whether a particular component is installed on a particular computer. A registry key value of 0x00000000 means the component is not installed, and a value of 0x00000001 means the component is installed.

Answer file entries and registry keys associated with IIS subcomponents for Windows 2000 Professional

IIS subcomponent	Answer file entry (in the [Components] section)	Registry key (for use in a script that checks whether a component is installed): 0x00000000 means it is not installed; 0x00000001 means it is installed
IIS common files	iis_common = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_common
IIS documentation	iis_doc = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_doc
File Transfer Protocol (FTP) service	iis_ftp = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_ftp
IIS MMC snap-in	iis_inetmgr = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_inetmgr
Personal Web Manager	iis_pwmgr = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_pwmgr
Simple Mail Transfer Protocol (SMTP) service	iis_smtp = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_smtp
Documentation for the	iis_smtp_docs = Off	No key available

Simple Mail Transfer Protocol (SMTP) service		
World Wide Web (WWW) service	iis_www = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_www
FrontPage server extensions	fp_extensions = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\fp_extensions

Procedures for checking or preventing the installation of IIS subcomponents

The following procedures explain how to:

- View the registry keys listed in the tables in the previous subsections
- View or change the IIS components currently installed on a computer running Windows 2000
- Prevent the installation of IIS subcomponents during unattended installation by using an answer file

To view registry keys related to IIS subcomponents

1. Open Registry Editor by clicking **Start**, clicking **Run**, and then typing **regedit**.

   Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

2. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\.
3. View the registry keys listed in the table in the previous subsections, and find the value associated with each key. A value of 0x00000000 means the component is not installed. A value of 0x00000001 means the component is installed.
4. Close Registry Editor.

To include or exclude IIS during Windows 2000 setup

1. During setup, when you see the Windows 2000 Components dialog box, scroll down to Internet Information Services (IIS).

   When the IIS component is selected, you can also click the **Details** button and view the check boxes for IIS subcomponents.

2. Select the check boxes for components you want to include.
3. Clear the check boxes for components you want to exclude.
4. Continue with setup.

To view or change the IIS components currently installed on a computer running Windows 2000

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Select Internet Information Services (IIS).
5. Perform one of the following steps:
   - If IIS is installed and you want to remove it, clear the check box for IIS and complete the wizard.
   - If IIS is not installed and you want to add it, select the check box for IIS and complete the wizard.
   - If you want to view the list of IIS subcomponents, after selecting IIS, click **Details**.

To prevent the installation of IIS subcomponents during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, ensure that you have the appropriate entries for excluding IIS from Windows 2000 Professional or from a product in the Windows 2000 Server family, as follows:
   - For a product in the Windows 2000 Server family, add the entries listed in the first table in this section, "Answer file entries and registry keys associated with IIS subcomponents for the Windows 2000 Server family." Ensure that all these entries specify **Off**.

     If IIS subcomponents are not listed in an answer file for unattended installation of a product in the Windows 2000 Server family, these subcomponents are installed by default. The exceptions are the FTP service and the Network News Transfer Protocol (NNTP) service, which are not installed by default.
   - For Windows 2000 Professional, ensure that there are no entries for the subcomponents listed in the second table in this section, "Answer file entries and registry keys associated with IIS subcomponents for Windows 2000 Professional." If you want to list any of these subcomponents, ensure that the entries specify **Off**.

     If IIS subcomponents are not listed in an answer file for unattended installation of Windows 2000 Professional, these subcomponents are *not* installed by default.

Internet Printing

This section provides information about:

- The benefits of Internet printing
- How Internet printing communicates with sites on the Internet
- How to control Internet printing to prevent the flow of information to and from the Internet

Benefits and purposes of Internet printing

Internet printing makes it possible for client computers running Microsoft Windows 2000 Service Pack 3 (SP3) to use printers located anywhere in the world by sending print jobs using Hypertext Transfer Protocol (HTTP).

Additionally, computers running Windows 2000 SP3 can use Microsoft Internet Information Services (IIS) or a Web peer server to create a Web page that provides information about printers and provides the transport for printing over the Internet.

Overview: Using Internet printing in a managed environment

You need to consider both the server and client components of Internet printing:

- Server: Internet Information Services 5.0 is installed by default on products in the Windows 2000 Server family with SP3. Although it is not installed by default on Windows 2000 Professional with SP3, it can easily be enabled. It is therefore possible for a user on a computer running Windows 2000 SP3 to configure that computer to act as a print server, allowing Internet printing. In a managed environment, you may want to remove IIS on any computers other than those specifically designated to service Internet traffic. On the computers running IIS, you may want to disable the Internet printing functionality of IIS, or at a minimum, properly secure IIS and Internet printing so that they are available only to authorized users.
- Client: Client computers can install an Internet printer using a Web browser, the Add Printer Wizard, or the Run dialog box. In order to prevent Internet printing, you must remove the ability for users to add an Internet printer.

Details on how to configure your Windows 2000 SP3 implementation to achieve these goals can be found later in this section.

How Internet printing communicates with sites on the Internet

The Internet printing process is as follows:

1. A user connects to a print server over the Internet by typing the URL for the print device.
2. The HTTP request is sent over the Internet to the print server.

3. The print server requires the client to provide authentication information. This ensures that only authorized users print documents on the print server.
4. After a user has authorized access to the print server, the server presents status information to the user by using Active Server Pages (ASP), which contain information about currently available printers.
5. When the user connects to any of the printers on the Internet printing Web page, the client computer first tries to find a driver for the printer locally. If an appropriate driver cannot be found, the print server generates a cabinet file (.cab file, also known as a Setup file) that contains the appropriate printer driver files. The print server downloads the .cab file to the client computer. The user on the client computer is prompted for permission to download the .cab file.
6. After users connect to an Internet printer, they can send documents to the print server by using Internet Printing Protocol (IPP).

Communication for Internet printing uses IPP and HTTP (or HTTPS) over any port that the print server has configured for this service. Because the service is using HTTP or HTTPS, this is typically port 80 or 443. Because Internet printing does support HTTPS traffic, communication can be encrypted, depending on the user's Internet browser settings.

Client computers running Windows 2000 SP3 can use Internet printing by default. Users must be authenticated by the print server, however, before they can use any of the printers connected to that server.

If IIS is installed on your computers running Windows 2000 SP3, Internet printing is automatically enabled as a feature of IIS. As described earlier, you can disable or restrict computers running Windows 2000 SP3 from hosting Internet printing through a variety of methods. See the following subsections for additional details.

The print server can use IIS and other technologies to collect and log extensive data about the user, the computer that sends the printing request, and the request itself. It is beyond the scope of this white paper to describe Web site operations and the specifics of what type of information can be collected. For more information about IIS and other related resources, see " Internet Information Services" in this white paper.

Controlling Internet printing to prevent the flow of information to and from the Internet

Client computers

To prevent the use of Internet printing from a client computer running Windows 2000 SP3, you can delete the registry key that the Print Spooler service uses to load the Internet print provider. The procedure for this method is provided in the next subsection.

How deleting the Internet print provider registry key can affect users and applications

Deleting the Internet print provider registry key on a client computer will prevent users of that computer from using Internet printing through the Run dialog box, the Add Printer Wizard, and the browser. Deleting this key, however, may also affect other print operations.

Print servers

As described earlier, users on a computer running a product in the Windows 2000 Server family with SP3 will, by default, also have IIS installed. Users on a computer running Windows 2000 Professional with SP3 might also have IIS installed. A computer with IIS installed can be configured to act as a print server, allowing Internet printing from other computers. In order to control this, you can use Group Policy to:

- Remove IIS from computers not specifically designated for use as an Internet server
- Disable Internet printing on computers that have IIS installed
- Restrict access to the printer to limited user IDs

Procedures for disabling Internet printing

Procedures for disabling Internet printing on a client computer running Windows 2000 SP3

To prevent users from using Internet printing on a client computer running Windows 2000 SP3, delete the Internet print provider registry key as described in the following procedure. This procedure must be performed on every computer running Windows 2000 SP3 in your organization for which you do not want to allow Internet printing. In order to ensure that these actions are correctly performed on all computers, consider using an automated setup routine or script.

To delete the Internet print provider registry key

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. Stop the Print Spooler service.
4. Use the Microsoft Registry Editor (Regedit.exe) to delete the following key from the registry:
5. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\Internet Print Provider
6. Restart the Print Spooler service.

Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

Procedures for disabling Internet printing on a computer running IIS

We recommend that you prevent users from installing IIS on computers not specifically designated as Internet servers. More details on how to achieve this can be found in "Internet Information Services" in this white paper.

For those computers that are running IIS, you can disable Internet printing if this is appropriate for your installation. The following procedure describes how to do this through Group Policy.

To disable Internet printing using Group Policy

1. On a computer running Windows 2000 SP3, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 SP3 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **Computer Configuration**, double-click **Administrative Templates**, and then click **Printers**.
3. In the details pane, double-click **Web-based Printing**.
4. Select **Disabled**.

Notes

This Group Policy setting is equivalent to setting the registry entry \\Hkey_Local_Machine\Software\Policies\Microsoft\Windows NT\Printers to DisableWebPrinters.

If you instead choose to allow Internet printing on your computers running IIS you should, at a minimum, strictly control who has access to your server's Internet printing Web site. For more information about the use of IIS in a controlled environment, see " Internet Information Services" in this white paper.

Related links

- For other procedures and best practices that can help you enhance the security of your Windows 2000 SP3 systems, see "Security Operations Guide for Windows 2000 Server" at:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/default.asp
- For general information about Group Policy, see Appendix B, "Resources for Learning About Group Policy."
- For more information about the use of IIS in a controlled environment, see "Internet Information Services" in this white paper.
- For more information about Internet printing, see the article "Overview of Internet Printing in Windows 2000" in the Microsoft Knowledge Base. You can search the Knowledge Base by going to:

  support.microsoft.com/

  and then following the instructions on the page. Search for "Internet printing."

Internet Protocol Version 6

This section provides the following information:

- A brief description of Microsoft IPv6 Technology Preview for Windows 2000
- References for more information about Internet Protocol version 6 (IPv6)

Microsoft IPv6 Technology Preview for Windows 2000

The Microsoft IPv6 Technology Preview for Windows 2000 (for Service Pack 1 or later) is a derivative of the Microsoft Research IPv6 Implementation, originally intended for application developers. It can be used to begin learning and experimenting with IPv6 where current implementations of IPv6 cannot be applied. Although there are no plans to release a production-quality version of IPv6 for Windows 2000, there is considerable documentation on the current and supported implementations of IPv6 at Microsoft. To view this documentation, click **Microsoft IPv6 Implementations** in the list of headings at this site:

www.microsoft.com/windowsserver2003/technologies/ipv6/

The IPv6 technologies can be present on a computer running Microsoft Windows 2000 Service Pack 3 (SP3) if you have installed the Microsoft IPv6 Technology Preview for Windows 2000 from the Microsoft Web site or from an alternate installation media source. If you have installed the Microsoft IPv6 Technology Preview for Windows 2000 and want to learn more about how to manage and configure IPv6, see "Internet Protocol Version 6 (IPv6)" on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/15_xpip6.asp

The technical description of Microsoft IPv6 technology and its related topics are beyond the scope of this white paper. For more information about Microsoft IPv6 technology, see the section on IPv6 in the white paper titled "Using Windows XP Professional with Service Pack 1 in a Managed Environment" on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

Related documentation and links

Web resources

- For more information about IPv6, see "Internet Protocol Version 6 (IPv6)" on the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/15_xpip6.asp

- For more information about Microsoft IPv6 technology, see the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

- For the most up-to-date information about Microsoft support for IPv6, and for a selection of white papers and other documentation, see the dedicated IPv6 Web site at:

  www.microsoft.com/ipv6

- For more information about the 6to4 tunneling technique, see "Connection of IPv6 Domains via IPv4 Clouds" in RFC 3056 on the IETF Web site at:

  www.ietf.org/rfc/rfc3056.txt?number=3056/

- For more general information about IP version 6, see the Microsoft Web site at:

  www.microsoft.com/windowsserver2003/technologies/ipv6/

- For more information about enterprise security, see "Best Practices for Enterprise Security" on the Microsoft Web site at:

  www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp

- For more information about IPv6 addressing, see "IP Version 6 Addressing Architecture" in RFC 2373 on the IETF Web site at:

  www.ietf.org/rfc/rfc2373.txt?number=2373/

- For the latest set of RFCs and Internet drafts describing IPv6/IPv4 coexistence and migration technologies, see the Next Generation Transition (ngtrans) Working Group Web site at:

  www.ietf.org/html.charters/ngtrans-charter.html

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Printed references

For more information about the IPv6 protocol suite, you can consult the following references:

- Davies, J. *Understanding IPv6.* Redmond, WA: Microsoft Press, 2002.
- Huitema, C. *IPv6: The New Internet Protocol.* Second edition. Upper Saddle River, NJ: Prentice Hall, 1998.
- Miller, M. *Implementing IPv6*: *Supporting the Next Generation of Protocols*. Second edition. Foster City, CA: M&T Books, 2000.

NetMeeting

This section provides information about:

- The benefits of NetMeeting
- Using NetMeeting in a managed environment
- How NetMeeting communicates with sites on the Internet
- How to control NetMeeting to limit the flow of information to and from the Internet

Benefits and purposes of NetMeeting

NetMeeting® conferencing software is a feature of Microsoft Windows 2000 Service Pack 3 (SP3) that enables real-time communication and collaboration over the Internet or an intranet. From a computer running the Windows 95, Windows 98, Windows NT® 4.0, Windows 2000, or Windows XP operating system, users can communicate over a network with real-time voice and video technology. Users can work together on virtually any Windows-based application, exchange or mark up graphics on an electronic whiteboard, transfer files, or use the text-based chat program.

NetMeeting helps small and large organizations take full advantage of their corporate intranet for real-time communications and collaboration. On the Internet, connecting to other NetMeeting users is made easy with Internet Locator Service (ILS), enabling participants to call each other from a dynamic directory within NetMeeting or from a Web page. New features include remote desktop sharing, virtual conferencing using Microsoft Outlook, new security features, and the ability to embed the NetMeeting user interface in an organization's intranet Web pages.

To learn more about the NetMeeting features, see the article on the Microsoft TechNet Web site at:

www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp

Overview: Using NetMeeting in a managed environment

NetMeeting supports communication standards for audio, video, and data conferencing. NetMeeting users can communicate and collaborate with users of other standards-based, compatible products. They can connect by modem, Integrated Services Digital Network (ISDN), or local area network (LAN) using Transmission Control Protocol/Internet Protocol (TCP/IP). In addition, support for Group Policy in NetMeeting makes it easy for administrators to centrally control and manage the NetMeeting work environment.

You can use Active Directory® directory service and Group Policy to configure NetMeeting to help meet your security requirements. You can also control the configuration of NetMeeting by using the NetMeeting Resource Kit. For more information about the NetMeeting Resource Kit, see "Alternate methods for controlling NetMeeting," later in this section.

NetMeeting components and features require that several ports be open from the firewall. For more information, see "NetMeeting and firewalls" later in this section.

How NetMeeting communicates with sites on the Internet

NetMeeting provides an infrastructure for communication between network applications and services. In this infrastructure, NetMeeting is both an application and a platform for other applications or services. The components and services in NetMeeting provide real-time communication and collaboration over the Internet or an organization's intranet.

NetMeeting audio and video conferencing features are based on the H.323 infrastructure, which enables NetMeeting to interoperate with other H.323 standards-based products. (H.323 is a standard approved by the International Telecommunication Union [ITU] that defines how audiovisual conferencing data is transmitted across networks.) NetMeeting data conferencing features are based on the T.120 infrastructure, enabling NetMeeting to interoperate with other T.120 standards-based products. (The T.120 standard is a suite of communication and application protocols developed for real-time, multipoint data connections and conferencing.)

Detailed information about the H.323 and T.120 standards is beyond the scope of this paper. Further information can be found on the following sites:

- For more information about the H.323 standard and NetMeeting, see "Understanding the H.323 Standard" at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part3/chaptr11.asp

- For more information about the H.323 specification, see the following Web sites at:

  www.itu.int/home/index.html

  www.imtc.org/h323.htm

- To learn more about the T.120 standard and NetMeeting, see "Understanding the T.120 Standard" at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part3/chaptr10.asp

- For more information about the T.120 architecture, see the International Multimedia Teleconferencing Consortium (IMTC) Web site at:

  www.imtc.org/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

NetMeeting port assignments

When you use NetMeeting to call other users over the Internet, several IP ports are required to establish the outbound connection. The following table describes the port numbers, their functions, and the resulting connection.

Port assignments for NetMeeting

Port	Function	Outbound connection
389	Internet Locator Service (ILS)	TCP
522	User Location Service (ULS)	TCP
1503	T.120	TCP

1720	H.323 call setup	TCP
1731	Audio call control	TCP
1024 through 65535 (dynamic)	H.323 call control	TCP
1024 through 65535 (dynamic)	H.323 streaming	Real-Time Transfer Protocol (RTP) over User Datagram Protocol (UDP)

For more information about NetMeeting communication ports and firewall configuration topics, see "Firewall Configuration" on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

Controlling NetMeeting to limit the flow of information to and from the Internet

You can configure NetMeeting by using Group Policy objects (GPOs) on servers running Windows 2000. (You can also control the configuration of NetMeeting by using the NetMeeting Resource Kit; for more information, see "Alternate methods for controlling NetMeeting," later in this section.)

This subsection includes information about the following topics:

- NetMeeting and Group Policy
- NetMeeting security
- NetMeeting and firewalls
- Establishing a NetMeeting connection with a firewall
- Firewall limitations for NetMeeting

NetMeeting and Group Policy

Group Policy can be used to define the default NetMeeting configuration settings that will be automatically applied to users and computers. These settings determine which NetMeeting features and capabilities are available to a particular group of users. The Group Policy configuration settings that are specific to NetMeeting are grouped into two different categories. These category groupings enable you to independently manage NetMeeting configuration settings for computers and users within your organization. Through the use of Group Policy you can enable, disable, or set configuration options for NetMeeting features or capabilities.

For additional information about Group Policy, see Appendix B, "Resources for Learning About Group Policy."

You can use Group Policy to manage the following NetMeeting configuration options for users in your organization:

- NetMeeting Group Policy settings for computers
- NetMeeting Group Policy settings for users

Configuring NetMeeting settings for computers through Group Policy

You can use Group Policy to determine the NetMeeting features and capabilities that are available to all users of the computers that are affected by the application of the NetMeeting Group Policy settings.

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. The NetMeeting Group Policy configuration setting that is specific to computers is as follows:

- **Disable remote Desktop Sharing**: You can use Group Policy to set remote desktop sharing choices in NetMeeting for the all users who are affected by the application of this Group Policy setting.

For more information about how to use Group Policy to manage the NetMeeting computer settings, see "To disable the NetMeeting remote desktop sharing feature through Group Policy" later in this section.

Note Computer-related Group Policy settings are applied when the operating system starts and during the periodic refresh cycle.

Configuring NetMeeting settings through Group Policy

You can use Group Policy to determine the NetMeeting features and capabilities that are available for a user or a group of users that are affected by the application of the NetMeeting Group Policy settings.

These Group Policy configuration options include the policy settings for NetMeeting, application sharing, audio and video, and the options page.

For more information about how to use Group Policy to manage the NetMeeting user settings, see "To disable the NetMeeting advanced calling feature through Group Policy" and "To disable the NetMeeting chat feature through Group Policy" later in this section.

The NetMeeting Group Policy configuration settings that are specific to users are as follows:

Configuring NetMeeting settings for users through Group Policy

For details about locating the Group Policy objects for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. You can use Group Policy to set configuration settings for the following NetMeeting features:

- **Enable Automatic Configuration**: Configures NetMeeting to download settings for users each time it starts.
- **Disable Directory services**: Disables the directory feature—users will not log on to a directory server when NetMeeting starts. Users will not be able to view or make calls using the NetMeeting directory.
- **Prevent adding Directory servers**: Prevents the user from adding directory servers to the list of available directory servers they can use for placing calls.
- **Prevent viewing Web directory**: Prevents the user from viewing directories as Web pages in a browser.

- **Set the intranet support Web page**: Sets the Web address that NetMeeting will display when users choose the Online Support command from the NetMeeting Help menu.
- **Set Call Security options**: Sets the level of security for outgoing and incoming NetMeeting calls.
- **Prevent changing Call placement method**: Prevents the user from changing the way calls are placed, either directly or by means of a gatekeeper server.
- **Prevent automatic acceptance of Calls**: Prevents the user from turning on automatic acceptance of incoming calls.
- **Allow persisting automatic acceptance of Calls**: Sets automatic acceptance of incoming calls to be persistent.
- **Prevent sending files**: Prevents users from sending files to others in a conference.
- **Prevent receiving files**: Prevents users from receiving files from others in a conference.
- **Limit the size of sent files**: Sets the maximum file size that can be sent to others in a conference.
- **Disable Chat**: Disables the chat feature of NetMeeting.
- **Disable NetMeeting 2.x Whiteboard**: Disables the NetMeeting 2.x Whiteboard feature. (The 2.x feature provides compatibility with older versions of NetMeeting only.)
- **Disable Whiteboard**: Disables the whiteboard feature of NetMeeting.

Configuring NetMeeting application sharing settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. You can use Group Policy to set configuration settings for the following elements of the NetMeeting Application Sharing feature:

- **Disable application Sharing**: Disables the NetMeeting application sharing feature completely. Users will not be able to host or view shared applications.
- **Prevent Sharing**: Prevents users from sharing anything themselves. They will still be able to view shared applications or desktops from others.
- **Prevent Desktop Sharing**: Prevents users from sharing their Windows desktop. They will still be able to share individual applications.
- **Prevent Sharing Command Prompts**: Prevents the user from sharing command prompts. Enabling this prevents the user from inadvertently sharing applications, since command prompts can be used to start other applications.
- **Prevent Sharing Explorer windows**: Prevents the user from sharing Windows Explorer windows. Enabling this prevents the user from inadvertently sharing applications, since Windows Explorer windows can be used to start other applications.
- **Prevent Control**: Prevents users from allowing others in a conference to control what they have shared. Enabling this enforces a read-only mode whereby the other participants cannot change the data in the shared application.
- **Prevent Application Sharing in true color**: Prevents users from sharing applications in true color, which uses more bandwidth.

Configuring NetMeeting audio and video settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. You can use Group Policy to set configuration settings for the following audio and video elements in NetMeeting:

- **Limit the bandwidth of Audio and Video**: Configures the maximum bandwidth, specified in kilobytes per second, to be used for audio and video.
- **Disable Audio**: Disables the audio feature of NetMeeting; users will not be able to send or receive audio.
- **Disable full duplex Audio**: Disables the full duplex audio mode. Users will not be able to listen to incoming audio while speaking into the microphone. Older audio hardware may not perform well when full duplex audio is enabled.
- **Prevent changing DirectSound Audio setting**: Prevents the user from changing the DirectSound audio setting. DirectSound has a better audio quality, although older audio hardware may not support it.
- **Prevent sending Video**: Prevents the user from sending video. Setting this option does not prevent the user from receiving video.
- **Prevent receiving Video**: Prevents the user from receiving video. Setting this option does not prevent the user from sending video.

Configuring NetMeeting options settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. You can use Group Policy to set configuration settings for the following elements of the NetMeeting Options page:

- **Hide the General page**: Removes the General tab on the NetMeeting Options page.
- **Disable the Advanced Calling button**: Disables the Advanced Calling button from the General page.
- **Hide the Security page**: Removes the Security tab on the NetMeeting Options page.
- **Hide the Audio page**: Removes the Audio tab on the NetMeeting Options page.
- **Hide the Video page**: Removes the Video tab on the NetMeeting Options page.

Note User-related Group Policy settings are applied when a user logs on to the computer and during the periodic refresh cycle.

To learn about specific Group Policy settings that can be applied to computers running Windows 2000 SP3, see the following spreadsheet, which lists policy settings for both Windows 2000 and Windows XP:

www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

NetMeeting security

The NetMeeting security architecture for data conferencing takes advantage of the existing, standards-compliant security features of Windows 2000 SP3 and Microsoft Internet Explorer. The

NetMeeting security architecture utilizes a 40-bit encryption technology and has the following security features:

- **Password protection**: This feature enables the user to create or participate in a meeting that requires a password to join. Password protection helps to ensure that only authorized users participate in a password-protected meeting. A password is also required to use the remote desktop sharing feature.
- **User authentication**: This feature provides a way to verify the identity of a caller or meeting participant using a personal or NetMeeting certificate.
- **Data encryption**: This feature helps to protect data exchanged during a meeting so that it is not easily read by any unauthorized parties that may intercept the data. The 40-bit data encryption applies to the whiteboard and chat features, shared applications, and transferred files. Audio and video communications are not encrypted.

NetMeeting security features integrate with security in Windows 2000 SP3 and Internet Explorer in the following ways:

- NetMeeting uses the NetMeeting private certificate store to provide personal certificates for user authentication and data encryption.
- NetMeeting uses the Windows certificate store to maintain NetMeeting certificates.
- NetMeeting uses the Crypto application programming interface (API) for certificate management and secure channels. (The Crypto API enables applications to encrypt or digitally sign data in a flexible manner while providing protection for private keys.)
- NetMeeting uses Security Support Provider Interface (SSPI) functions to generate and process security tokens.

These security features can be implemented by an administrator or a NetMeeting user. Using the NetMeeting Resource Kit Wizard or Group Policy in NetMeeting, the administrator can enforce security settings that apply to all users. If allowed by the administrator, NetMeeting users can also select their own security settings in the NetMeeting user interface (UI) and change security settings for individual calls.

You can use the following sources to learn more about NetMeeting configuration and security topics:

- For more information about the NetMeeting Resource Kit Wizard, see the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter2.asp
- For more information about Kerberos authentication, see "The Kerberos Network Authentication Service (V5)" (RFC 1510) on the IETF Web site at:

  www.ietf.org/rfc/rfc1510.txt

  (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)
- For more information about the security features available in NetMeeting, see the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter5.asp

NetMeeting and firewalls

You can configure firewall components in a variety of ways, depending on your organization's specific security policies and overall operations. While most firewalls are capable of allowing primary (initial) and secondary (subsequent) Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections, it is possible that they are configured to support only specific connections based on security considerations. For example, some firewalls support only primary TCP connections, which some professionals view as the most reliable.

For NetMeeting multipoint data conferencing—program sharing, whiteboard, chat, file transfer, and directory access—your firewall only needs to pass through primary TCP connections on assigned ports. NetMeeting audio and video features require secondary TCP and UDP connections on dynamically assigned ports.

Note NetMeeting audio and video features require secondary TCP and UDP connections. Therefore, when you establish connections through firewalls that accept only primary TCP connections, you are not able to use the audio or video features of NetMeeting.

Detailed firewall configuration procedures for NetMeeting are beyond the scope of this white paper. For more information about NetMeeting firewall connections, see the NetMeeting 3 Resource Kit, specifically, the section titled "Establishing a NetMeeting Connection with a Firewall" in the "Firewall Configuration" chapter on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

Microsoft NetMeeting can be configured to work with an organization’s existing firewall security. Because of limitations in most firewall technology, however, few products are available that enable you to securely transport inbound and outbound NetMeeting calls containing audio, video, and data across a firewall. You should consider carefully the relative security risks of enabling different parts of a NetMeeting call in your firewall product. You must especially consider the security risks involved when modifying your firewall configuration to enable any component of an inbound NetMeeting call.

Some organizations have security or policy concerns that require them to limit how fully they support NetMeeting in their firewall configuration. These concerns are based on network capacity planning or weaknesses in the firewall technology being used. For example, security concerns might prohibit an organization from accepting any inbound or outbound flow of UDP data through the firewall. Because these UDP connections are required for NetMeeting audio and video features, disabling this function excludes audio and video features in NetMeeting for calls through the firewall. The organization can still use NetMeeting data conferencing features such as program sharing, file transfer, whiteboard, and chat for calls through the firewall by allowing only TCP connections on ports 522 and 1503.

For more information about NetMeeting firewall security, see the NetMeeting 3 Resource Kit, specifically, the section titled "Security and Policy Concerns" in the "Firewall Configuration" chapter on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

Establishing a NetMeeting connection with a firewall

When you use NetMeeting to call other users over the Internet, several IP ports are required to establish the outbound connection.

If you use a firewall to connect to the Internet, it must be configured so that the following IP ports are not blocked:

- TCP ports 389, 522, 1503, 1720, and 1731
- TCP and UDP ports (1024 through 65535)

To establish outbound NetMeeting connections through a firewall, the firewall must be configured to do the following:

- Pass through primary TCP connections on ports 389, 522, 1503, 1720, and 1731
- Pass through secondary TCP and UDP connections on dynamically assigned ports (1024 through 65535)

The H.323 call setup protocol dynamically negotiates a TCP port for use by the H.323 call control protocol. Also, both the audio call control protocol and the H.323 call setup protocol dynamically negotiate UDP ports for use by the H.323 streaming protocol, called the Real-Time Transfer Protocol (RTP). In NetMeeting, two UDP ports are designated on each side of the firewall for audio and video streaming, for a total of four ports for inbound and outbound audio and video. These dynamically negotiated ports are selected arbitrarily from all ports that can be assigned dynamically.

NetMeeting directory services require either port 389 or port 522, depending on the type of server you are using. The Microsoft Internet Locator Service (ILS), which supports LDAP for NetMeeting, requires port 389. The Microsoft User Location Service (ULS), developed for NetMeeting 1.0, requires port 522.

Firewall limitations for NetMeeting

Some firewalls cannot support an arbitrary number of virtual internal IP addresses, or cannot do so dynamically. With these firewalls, you can establish outbound NetMeeting connections from computers inside the firewall to computers outside the firewall, and you can use the audio and video features of NetMeeting. Users outside the organization cannot, however, establish inbound connections from outside the firewall to computers inside the firewall. Typically, this restriction is due to limitations in the network implementation of the firewall.

> **Note** Some firewalls are capable of accepting only certain protocols and cannot handle TCP connections. For example, if your firewall is a Web proxy server with no generic connection-handling mechanism, you will not be able to use NetMeeting through the firewall.

You can use the following sources to learn more about NetMeeting configuration and firewall topics:

- For more information about NetMeeting firewall connections, see the NetMeeting 3 Resource Kit, specifically, the section titled "Establishing a NetMeeting Connection with a Firewall" in the "Firewall Configuration" chapter on the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

- For more information about using NetMeeting and your firewall, see "How to Establish NetMeeting Connections through a Firewall" on the Microsoft Web site at:

  support.microsoft.com/default.aspx?scid=KB;en-us;Q158623

Alternate methods for controlling NetMeeting

You can create customized installation options for specific users or groups within your organization by using the NetMeeting Resource Kit Wizard. Additionally, you can use the NetMeeting Resource Kit Wizard to control user and computer access rights by creating custom configurations of client settings and specific features that you have selected to restrict or allow. For example, you can control audio and video access, set data throughput limits and network speeds, and choose to display online support. The Resource Kit Wizard can also help you set up various configurations of NetMeeting for different types of users and different levels of security. It can help you save network bandwidth by restricting specific features. You can also use the Resource Kit Wizard to both change registry settings for all NetMeeting users, and to implement such changes globally.

> **Note** By selecting certain options in the Resource Kit Wizard, be aware that you may be changing the NetMeeting user interface. For example, if you click **Restrict the Use of Video**, the Video tab doesn't appear in the NetMeeting user's Options dialog box.

The Resource Kit for NetMeeting has a section that provides detailed information about responding to NetMeeting problems, including problem descriptions, causes, and resolutions. For more information about the NetMeeting 3 Resource Kit, see Windows NetMeeting 3 Resource Kit on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/nm3dldoc.asp

Procedures for configuration of NetMeeting

NetMeeting is designed to enhance the enterprise environment and enable users to communicate internally and externally with other NetMeeting users. You can use Group Policy to develop a NetMeeting feature management policy to support the specific business rules or communication policies that exist within your organization. For example, your organization may not want users to be able to access or use the NetMeeting chat feature from their computers. By using Active Directory and Group Policy, you can disable the chat feature from any or all computers that are affected by the application of the Group Policy configuration settings.

For lists of Group Policy settings that you can use to manage NetMeeting configuration options, see "NetMeeting and Group Policy" earlier in this section.

Procedures for managing NetMeeting features through Group Policy

This subsection provides procedures for the following configuration methods:

- Locating the Group Policy objects (GPOs) for NetMeeting configuration settings. These are the settings listed in "NetMeeting and Group Policy" earlier in this section.
- Disabling the NetMeeting remote desktop sharing feature. This prevents users from using this feature.
- Disabling the NetMeeting advanced calling feature on the NetMeeting options page.
- Disabling the NetMeeting chat feature.

To locate the Group Policy objects (GPOs) for NetMeeting user configuration settings

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. View the Group Policy objects that are available. For more information about these objects, see "NetMeeting and Group Policy" earlier in this section.

To locate the Group Policy objects (GPOs) for NetMeeting computer configuration settings

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. View the Group Policy objects that are available. For more information about these objects, see "NetMeeting and Group Policy" earlier in this section.

To disable the NetMeeting remote desktop sharing feature through Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. In the details pane, double-click **Disable remote Desktop Sharing**.
4. Select **Enabled**.

   Note Computer-related Group Policy settings are applied when the operating system starts and during the periodic refresh cycle.

To disable the NetMeeting advanced calling feature through Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."

2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, click **NetMeeting**, and then click **Options Page**.
3. In the details pane, double-click **Disable the Advanced Calling button**, and then select **Enabled.**

To disable the NetMeeting chat feature through Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. In the details pane, double-click **Disable Chat**, and then select **Enabled**.

Related links

Web resources

- For more information about using NetMeeting and your firewall, see "How to Establish NetMeeting Connections through a Firewall" on the Microsoft Web site at:

  support.microsoft.com/default.aspx?scid=KB;en-us;Q158623

- For more information about NetMeeting, see Windows NetMeeting on the Microsoft Web site at:

  www.microsoft.com/windows/NetMeeting/

- For more information about configuring NetMeeting, see the Windows NetMeeting Resource Kit on the Microsoft Web site at:

  www.microsoft.com/windows/NetMeeting/Corp/ResKit/

- To learn more about NetMeeting features, see the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp

- To view articles that explain how to use some of the new features in NetMeeting, see the Microsoft Web site at:

  support.microsoft.com/default.aspx?scid=/support/netmeeting/howto/default.asp

- For more information about Kerberos authentication, see "The Kerberos Network Authentication Service (V5)" (RFC 1510) on the Internet Engineering Task Force (IETF) Web site at:

  www.ietf.org/rfc/rfc1510.txt

- For more information about the H.323 specification, see the ITU-T Web site at:

  www.itu.int/home/index.html

- For more information about the T.120 architecture, see the International Multimedia Teleconferencing Consortium (IMTC) Web site at:

www.imtc.org/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Printed references

For more information about firewall design, policy, and security considerations for firewall design in general, you can consult the following reference:

- Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly & Associates, Inc., 1995.

Outlook Express (Included in Internet Explorer)

The subsections that follow provide:

- A description of Microsoft Outlook Express, which is included in Microsoft Internet Explorer, and a comparison of Outlook® and Outlook Express.

  The version of Outlook Express described in this paper is 5.50.4807.1700, the version included in Microsoft Windows 2000 Service Pack 3 (SP3). You can view the version number by starting Outlook Express, clicking **Help**, and clicking **About Outlook Express**.

  At the end of this section of the white paper, there are links to information about Internet Explorer 6 SP1, which includes Outlook Express 6 SP1 and is readily available for downloading. If you are deploying Windows 2000 SP3 across an organization, we recommend that you consider including Internet Explorer 6 SP1 (which includes Outlook Express 6 SP1) in your deployment, because of the additional security-related options and settings available in that version. If you include Internet Explorer 6 SP1 in your deployment, the required order for downloading is Windows 2000 SP3 first and Internet Explorer 6 SP1 second (restarting after each download).

- Descriptions of the security zones in the version of Outlook Express in Windows 2000 SP3, with information about how they are configured at the desktop.

- Information about removing all visible entry points to Outlook Express in Windows 2000 Professional with SP3, for situations where you want users to use another e-mail client exclusively. There are several ways to do this:

  - During unattended installation when you use the integrated installation method for SP3, which enables you to simultaneously install Windows 2000 and the service pack.

  - Through Add/Remove Programs in Control Panel.

  - With **Set Program Access and Defaults**, which is available from the Start menu on Windows 2000 Professional with SP3. With this dialog box, the administrator of a computer running Windows 2000 Professional with SP3 can specify which e-mail program is shown on the Start menu, desktop, and other locations.

Note This section of the white paper describes Outlook Express, but it does not describe Internet Explorer (of which Outlook Express is part) or the Internet Connection Wizard. For information about these components, see the respective sections of this white paper.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization where users send e-mail, receive e-mail, open attachments in e-mail, and perform similar actions. This section, however, provides information about features and configuration methods in this version of Outlook Express that can reduce the inherent risks associated with sending and receiving e-mail.

For more information about Outlook Express, see the following resources:

- Help for Outlook Express (which can be accessed in Outlook Express by clicking the **Help** menu and then selecting an appropriate option).

- The section about Internet Explorer in this white paper, which describes security zones in Internet Explorer. These security zones are also used in the version of Outlook Express in Windows 2000 SP3.

- The Internet Explorer page on the Microsoft Web site at:

  www.microsoft.com/windows/ie/

- The Resource Kit for Internet Explorer (specifically, the chapter describing what's new in Internet Explorer 5). To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

  www.microsoft.com/reskit/

Benefits and purposes of Outlook Express

Outlook Express is designed to make it easy to send or receive e-mail and to browse or participate in newsgroups. It differs from many of the other components described in this white paper in that its main function is to communicate through the Internet or an intranet (in contrast to components that communicate with the Internet in the process of supporting some other activity).

Outlook Express is part of Internet Explorer, in contrast to Microsoft Outlook, which is an application included in Microsoft Office. Outlook provides comprehensive e-mail capabilities, including information management and collaboration capabilities, useful to a wide spectrum of users from home to small business to large enterprise. Outlook Express, included as part of Internet Explorer, offers standard Internet e-mail and news access, useful to many home and small-business users. Outlook Express supports Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP).

The version of Outlook Express in Windows 2000 SP3 can be run in either of two security zones. These security zones are configured in Internet Explorer (described in the corresponding section in this white paper). The following subsections explain how to specify the security zone to be used for Outlook Express, and they outline methods for removing all visible entry points to Outlook Express in Windows 2000 SP3 (for situations where you want users to use another e-mail client exclusively).

Security zones in Outlook Express in Windows 2000 SP3

The version of Outlook Express in Windows 2000 SP3 can be run in either of two security zones. These security zones are configured in Internet Explorer. The two security zones that you choose between in Outlook Express are as follows.

> **Note** For information about the security zones in Internet Explorer, see the Internet Explorer section of this white paper.

- Internet zone: With this setting, Outlook Express uses the same security level as the one that you set for the Internet zone in Internet Explorer.
- Restricted sites: With this setting, Outlook Express uses the same security level as the one that you set for the Restricted sites zone in Internet Explorer.

For a procedure that tells how to view or specify the security zone to be used for Outlook Express, see "Procedures for working with Outlook Express in Windows 2000 SP3" later in this section.

Overview: Using Outlook Express with Windows 2000 SP3 in a managed environment

Although there are inherent risks associated with sending and receiving e-mail (and e-mail attachments), you can reduce the risks by using the following options in the version of Outlook Express found in Windows 2000 SP3:

- You can configure appropriate settings for security zones in Internet Explorer and Outlook Express. For more information, see "Security zones in Outlook Express in Windows 2000 SP3" earlier in this section and "To start Outlook Express and view or specify the security zone" later in this section.
- You can ensure that all visible entry points to Outlook Express in Windows 2000 SP3 are removed (for situations where you want users to use another e-mail client exclusively). For more information, see "Removing visible entry points to Outlook Express during deployment of Windows 2000 SP3" and "Procedures for working with Outlook Express in Windows 2000 SP3" later in this section.

Removing visible entry points to Outlook Express during deployment of Windows 2000 SP3

For situations where you always want users to use an e-mail client other than Outlook Express, you can remove all visible entry points to Outlook Express in Windows 2000 SP3. One way to do this is during workstation or server deployment by using standard methods for unattended installation or remote installation. If you are using an answer file, the entry is as follows:

```
[Components]
OEAccess = Off
```

Note You can use OEAccess in an answer file only if you are using the integrated installation method for SP3, which enables you to simultaneously install Windows 2000 and the service pack. If you plan to install Windows 2000 by itself and then later apply SP3, you cannot use OEAccess in an answer file. For more information about the integrated installation methods for SP3, see the Service Pack 3 Installation and Deployment Guide at the following Web site:

www.microsoft.com/windows2000/downloads/servicepacks/sp3/spdeploy.htm

For more information about unattended installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."

For information about specifying which e-mail program is shown on the Start menu, desktop, and other locations and about removing all visible entry points to Outlook Express on an individual computer, see the next subsection, "Procedures for working with Outlook Express in Windows 2000 SP3."

Procedures for working with Outlook Express in Windows 2000 SP3

This subsection provides procedures for the following tasks:

- Opening the dialog box from which you can view or specify the security zone setting for Outlook Express.
- Specifying which e-mail program is shown on the Start menu, desktop, and other locations on a computer running Windows 2000 Professional with SP3. You can do this through **Set Program Access and Defaults** on the Start menu.
- Removing visible entry points to Outlook Express on an individual computer running Windows 2000 Professional SP3.
- Removing visible entry points to Outlook Express during unattended installation of Windows 2000 SP3 by using an answer file.

To start Outlook Express and view or specify the security zone

1. Click **Start**, point to **Programs**, and then click **Outlook Express**.
2. On the **Tools** menu, click **Options**.
3. Click the **Security** tab and view or specify the security zone.

   When you specify a security zone, Outlook Express uses the same security level as the one that you set for that zone in Internet Explorer. For more information about security zones, see the section about Internet Explorer in this white paper.

To specify which e-mail program is shown on the Start menu, desktop, and other locations on a computer running Windows 2000 Professional with SP3

To perform the following procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.

Note **Set Program Access and Defaults** appears on Windows 2000 Professional with SP3 only. It does not appear on Windows 2000 Server with SP3, Windows 2000 Advanced Server with SP3, or Windows 2000 Datacenter with SP3.

---

1. Click **Start** and then click **Set Program Access and Defaults**.
2. Select the default e-mail program from the options available.

Note If your program does not appear by name, close the **Set Program Access and Defaults** interface and configure your e-mail program as the default program. Then open **Set Program Access and Defaults** and click **Use my current e-mail program**. For information about how to configure a program to be the default, contact the vendor of that program. Also, for information about the coding that enables an e-mail program to be configured as the default, see the Microsoft Developer Network Web site at:

msdn.microsoft.com/library/en-us/shellcc/platform/shell/programmersguide/shell_adv/registeringapps.asp

---

3. Select the **Show this program** check box.

For more information about **Set Program Access and Defaults**, see the Microsoft Product Support Services Web site at:

support.microsoft.com/default.aspx?scid=kb%3ben-us%3b327931

To remove visible entry points to Outlook Express on an individual computer running Windows 2000 Professional SP3

To perform the following procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Scroll down the list of components to Outlook Express, and make sure the check box for that component is cleared.
5. Follow the instructions to complete the Windows Components Wizard.

To remove visible entry points to Outlook Express during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, include the following entry:

   OEAccess = Off

   Note You can use OEAccess in an answer file only if you are using the integrated installation method for SP3, which enables you to simultaneously install Windows 2000 and the service pack. If you plan to install Windows 2000 by itself and then later apply SP3, you cannot use OEAccess in an answer file. For more information about the integrated installation methods for SP3, see the Service Pack 3 Installation and Deployment Guide at the following Web site:

   www.microsoft.com/windows2000/downloads/servicepacks/sp3/spdeploy.htm

Related links: Information about Internet Explorer 6 SP1 and Outlook Express 6 SP1

Outlook Express 6 SP1 is part of Internet Explorer 6 SP1, which is readily available for downloading. If you are deploying Windows 2000 SP3 across an organization, we recommend that you consider including Internet Explorer 6 SP1 in your deployment (instead of the version of Internet Explorer included in Windows 2000 SP3), because Internet Explorer 6 SP1 offers additional security-related options and settings. If you include Internet Explorer 6 SP1 in your deployment, the required order for downloading is Windows 2000 SP3 first and Internet Explorer 6 SP1 second (restarting after each download).

The following list provides sources of information about Internet Explorer 6 SP1 and Outlook Express 6 SP1:

- The Internet Explorer Web site at:

  www.microsoft.com/windows/ie/

- The Outlook Express section in the white paper titled "Using Windows XP Professional with Service Pack 1 in a Managed Environment." This paper can be found on the Technet Web site at:

  www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

- Help for Outlook Express: after downloading Internet Explorer (which includes Outlook Express), start **Outlook Express**, click the **Help menu**, and then select an appropriate option.

- The Resource Kit for Internet Explorer. To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

  www.microsoft.com/reskit/

Registration Wizard

This section provides the following information:

- A brief description of the Registration Wizard in Microsoft Windows 2000 Service Pack 3 (SP3), and how it communicates with sites on the Internet
- How to control the Registration Wizard to limit the flow of information to and from the Internet

Purposes of the Registration Wizard

With the Registration Wizard, a user or administrator can register Windows 2000 directly through the Internet, instead of mailing in a card. Product registration involves the provision of personally identifiable information, such as an address, to Microsoft for the purpose of receiving information about product updates and special offers. Registration is usually done on a per-product basis and is not required. If registration is completed, all registration information is stored using a variety of security technologies and is never loaned or sold outside Microsoft.

The Registration Wizard is designed to be easy to start immediately after setup of Windows 2000. At that time, one of the following interfaces appears:

- **On a client**: Getting Started with Windows 2000
- **On a server**: Configure Your Server

In either of these interfaces in Windows 2000, clicking **Register Now** starts the Registration Wizard.

The Registration Wizard can be started from the command line (if it has not previously been run) on any computer running Windows 2000 by opening a command prompt and typing the following command:

regwiz /r

Overview: Product registration in a managed environment

If a user of a newly installed computer chooses to run the Registration Wizard and has Internet access, the wizard will communicate with the registration site at Microsoft. As an administrator, you can control this by using Group Policy to prevent users from running the Registration Wizard (that is, you can add Regwiz.exe to a list of Windows applications that cannot be run). For more information, see "Procedure for using Group Policy to prevent users from starting the Registration Wizard" later in this section.

How a computer communicates with sites on the Internet during registration

Windows 2000 can be registered through the Internet or by mailing in a card from the product package. Registration is optional. If Windows 2000 is registered through the Internet, it communicates with Web sites as follows:

- **Specific information sent or received**: During Internet-based registration of Windows 2000, the person carrying out registration can send the following to the registration server at Microsoft:
  - **Place where operating system is used**: The two choices are "Home" and "Work."
  - **Name**: First and last name are required for completing registration (registration itself is optional).
  - **Company** (can be filled in only if "Work" is selected as the place of use): Required for completing registration (registration itself is optional).
  - **Address**: Required for completing registration (registration itself is optional).
  - **Telephone number**: Optional.
  - **User role**: Optional. If "Home" was selected in a previous page, an optional user questionnaire is offered, with rating scales to indicate the person's level of interest in computers. If "Work" was selected in a previous page, a list is offered for making an optional choice of role, for example, "IT Decision-maker" or "General Business user."
  - **Permission to share mailing information with partners that Microsoft works with**: Occasionally, Microsoft allows carefully selected partners to offer its customers products and services by mail. The person registering can permit or prevent this sharing.
  - **System inventory information**: The Registration Wizard takes an inventory of the system hardware (devices) and the operating system software. The person registering the product decides whether to submit the inventory with the registration. Submitting the inventory helps Microsoft understand which devices are in use, which in turn helps Microsoft to provide better customer support and to improve future products.
- **Default setting**: By default, the Registration Wizard can be run.
- **Trigger and user notification**: The person at the computer triggers the starting of the Registration Wizard by clicking **Register Now** in one of the interfaces described in the preceding subsection, or by typing **regwiz /r** as described in "Purposes of the Registration Wizard" earlier in this section. Before the wizard starts and in the first page of the wizard, brief explanations notify the person that completing the wizard will cause the product to be registered.
- **Logging**: There is no logging of the registration process.
- **Privacy, access, and storage**: Registration data, which contains information that the person registering the product chooses to send to Microsoft, is stored on servers with limited access that are located in controlled facilities. Registration data can be seen by customer service representatives and marketing personnel.

  To review the Microsoft online privacy statement on registration, see the following Web site at:

  www.microsoft.com/info/privacy.htm
- **Transmission protocol and port**: Any registration data that is sent uses HTTP through port 80.
- **Ability to disable**: To disable the Registration Wizard, see "Procedure for using Group Policy to prevent users from starting the Registration Wizard" later in this section.

Procedure for using Group Policy to prevent users from starting the Registration Wizard

You can use Group Policy to prevent users from starting the Registration Wizard, that is, you can add Regwiz.exe to a list of Windows applications that cannot be run.

To prevent users from starting the Registration Wizard by using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
3. In the details pane, double-click **Don't run specified Windows applications**.
4. Select **Enabled**, click **Show**, click **Add**, and then enter the application executable name, Regwiz.exe.

Search Assistant

This section provides information about:

- The benefits of Search Assistant
- How Search Assistant communicates with sites on the Internet
- How to control Search Assistant to prevent the flow of information to and from the Internet

Benefits and purposes of Search Assistant

Search Assistant in Microsoft Windows 2000 Service Pack 3 (SP3) enables users to search for files and folders on their desktop computer, to search for files, people, and other computers on their internal network, and to search for information on the Internet. Search Assistant uses Indexing Service to maintain an index of all the files on users' computers, making searches faster.

When employing Search Assistant, users can specify several search criteria. For example, they can search for files and folders by name, type, or size. They can find files based on when they were last modified, or search for files containing specific text.

Overview: Using Search Assistant in a managed environment

Search Assistant is a feature of Microsoft Internet Explorer and directs users to various kinds of information sources on the Internet including dictionaries, map engines, and Web site directories.

When the user searches the Internet using Search Assistant, the information collected consists only of the text of the search query. Search Assistant does not collect any personal or demographic information.

Microsoft does not use the information collected to identify the user individually and it does not use the information in conjunction with other data sources that may contain personal data. Microsoft does not collect information when the user searches on the local system, local area network (LAN), or intranet.

In a managed environment, you may want to limit user access to the Internet. You can limit user access by disabling Search Assistant through Group Policy. This procedure is given later in this section.

How Search Assistant communicates with sites on the Internet

Search Assistant can only access the Microsoft Network (MSN®) search engine when there is Internet connectivity; users are neither required nor prompted to connect to the Internet. When users navigate to Start\Search\On the Internet and select the **Find a Web site** option from the

search options list, they are taken to search.msn.com. From there the user has access to other pages and sites within MSN.com and to the Internet.

Search Assistant uses HTTP protocol over port 80 to communicate. It does not log or encrypt any data. The feature can be disabled by removing the search option from the Start menu through Group Policy as described in the following subsection.

Controlling Search Assistant to prevent the flow of information to and from the Internet

You can disable Search Assistant by removing the search option from both the Start menu and the toolbar in Windows Explorer through the use of Group Policy settings.

To remove the Search menu from the Start menu

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, and then click **Start Menu & Taskbar**.
3. In the details pane, double-click **Remove Search menu from Start menu**.
4. Select **Enabled**.

Terminal Services Licensing

This section provides information about:

- The purposes of Terminal Services Licensing
- How Terminal Services Licensing communicates with sites on the Internet
- How to control Terminal Services Licensing to limit the flow of information to and from the Internet

Purposes of Terminal Services Licensing

Terminal Services Licensing is the client license management component for the Microsoft Windows 2000 Server family with Service Pack 3 (SP3). (Terminal Services Licensing is not included with Windows 2000 Professional.) If you install Terminal Services in application server mode (not remote administration mode), so that users can use applications directly from servers, you must also install Terminal Services Licensing, although not necessarily on the same server. Temporary licenses can be issued for dients that enable them to use Terminal servers for up to 90 days.

Terminal Services and Terminal Services Licensing are optional components that you can install on any product in the Windows 2000 Server family. When you set up Terminal Services in application server mode on a server running Windows 2000, users can access applications running on Terminal servers, thereby enabling them to run the applications you provide, regardless of the type of hardware or operating system on their computers. For descriptions of other ways you can use Terminal Services, see the Terminal Services overviews on the Microsoft Web site at:

www.microsoft.com/windows2000/technologies/terminal/default.asp

For details about the licenses necessary with Terminal Services, see the Windows 2000 Web site at:

www.microsoft.com/windows2000/docs/tslicensing.doc

Overview: Using Terminal Services Licensing in a managed environment

You can control the communication that occurs between the Terminal Services Licensing component and sites on the Internet by choosing the server or servers on which to install the Terminal Services Licensing component, and by choosing among four methods for activation. (You also choose among the same four methods for obtaining client license key packs, which are digital representations of a group of client access licenses.) The four methods for activation are as follows:

- Direct Internet
- Internet communication from a computer other than the one where Terminal Services Licensing is installed

- Phone
- Fax

For more details on these methods, see the subsections that follow.

How Terminal Services Licensing communicates with sites on the Internet

A server running the Terminal Services Licensing component communicates with the Microsoft Clearinghouse (a database for managing licensing) on the Internet only when you activate Terminal Services Licensing or when you initiate subsequent transactions with Microsoft to obtain client license key packs. The following list describes the communication that occurs when you activate or obtain client license key packs directly over the Internet or when you connect to the Microsoft Clearinghouse from a computer other than the one where Terminal Services Licensing is installed.

Notes

The information in the following list applies only to activation or obtaining client license key packs over the Internet. It does not apply when you activate by phone or by fax.

Activation by phone and fax are done as follows: When you activate by phone, you start the Licensing Wizard, choose a country or region from the list that is displayed, and call the number shown. When you activate by fax, you start the Licensing Wizard to generate a page containing the necessary activation or license installation information, fax it to the Microsoft Customer Service Center, and receive a reply from Microsoft by fax. (A return fax number is required for activation by fax.)

The rest of this subsection describes various aspects of the data that is sent to and from the Internet through Terminal Services Licensing and how the exchange of information takes place.

- **Specific information sent or received**: The information sent to the Microsoft Clearinghouse includes company name, first and last name of the user, license server name, and license server ID. Client license key packs are returned to the Terminal Services license server.
- **Default settings**: Terminal Services Licensing is not installed by default.
- **Trigger and user notification**: The administrator triggers activating, obtaining client license packs, or deactivating Terminal Services Licensing by performing the steps described in "Procedures for configuration of Terminal Services Licensing," later in this section. When the Terminal Services Licensing component starts, the administrator is notified that activating, obtaining client license packs, or deactivating will initiate communication with Microsoft.
- **Logging**: Terminal Services Licensing logs events in the system log. The events can be viewed through Event Viewer.
- **Encryption**: Terminal Services Licensing uses the HTTP protocol over SSL (Secure Sockets Layer) to communicate on the Internet and the Web.
- **Access**: The Microsoft Clearinghouse is the database Microsoft maintains to activate license servers and to issue client license key packs. Microsoft customer service representatives have access to the licensing information and are able to successfully re-create the information on your Terminal Services license server if technical problems occur. The information you provide might also be used internally at Microsoft to perform aggregate quality testing of the Terminal Services Licensing program.

- **Privacy policy**: For information on Microsoft's privacy policy for Terminal Services Licensing see the following sources:
  - Search for "Terminal Services Privacy" in Windows 2000 Help at:

    www.microsoft.com/windows2000/en/server/help/default.asp?url=/WINDOWS2000/en/server/help/ts_lice_c_070.htm
  - The Terminal Services Licensing Web site, where you can click the privacy shortcut:

    https://activate.microsoft.com/
- **Transmission protocol and port**: The port used by the HTTPS protocol is TCP 443, and the port used by the remote procedure call (RPC) protocol is TCP 135.
- **Ability to disable**: Terminal Services Licensing is not installed by default. Once installed, however, it can be disabled by the procedures described later in this section.

Terminal Services Internet Connector Licensing

In place of individual Terminal Services Client Access Licenses (TS CALs), you have the option of purchasing the Windows 2000 Terminal Services Internet Connector license. This license allows a maximum of 200 concurrent users to connect anonymously to a Terminal server over the Internet. This is useful for organizations that want to demonstrate Windows-based software to Internet users without rewriting Windows-based applications as Web applications. Any user who accesses a Terminal server with this license must not be an employee.

When you use the Internet Connector license with a specific server running Windows 2000, Terminal Services only allows anonymous client access. You cannot use the Internet Connector license with other types of Terminal Services client access licenses on the same server running Windows 2000.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running servers that communicate with the Internet. For more information about security and the Internet, see the introduction to this white paper, or search for "Internet connector" in the documents on the following Microsoft Web sites at:

- www.microsoft.com/windows2000/docs/tslicensing.doc
- www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/part4/chapt-16.asp

Controlling Terminal Services Licensing to limit the flow of information to and from the Internet

You can control the communication that occurs between the Terminal Services Licensing component and sites on the Internet in the following ways:

- **Install the Terminal Services Licensing component on selected servers only**. This follows the basic principle of stopping unnecessary services and keeping computers (especially servers) free of unnecessary software. For information about choosing which computer or computers on which to install Terminal Services Licensing, see the Windows 2000 Server Deployment Planning Guide, which is available on the Microsoft Web site at:

www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/part4/chapt-16.asp

In the chapter in the preceding link, search for "domain license server" and "enterprise license server" for information about factors to consider when choosing which computer or computers on which to install Terminal Services Licensing.

- **Review the method you want to use for activating Terminal Services Licensing before starting the Licensing Wizard**. Direct Internet activation is the fastest method, but if you prefer, you can activate by the other methods mentioned previously (connecting to a Web site from a computer other than the one where Terminal Services Licensing is installed, activating by phone, or activating by fax).

  You are required to activate a license server before it can issue licenses to Terminal Services clients. You are required to activate a license server only once. When you activate the license server, Microsoft provides the server with a limited-use digital certificate that validates server ownership and identity. Microsoft uses the X.509 industry standard certificate for this purpose. Using this certificate, a license server can make subsequent transactions with Microsoft and receive client license key packs.

Procedures for configuration of Terminal Services Licensing

Terminal Services Licensing servers can be configured in several ways as described previously. This subsection provides procedures for:

- Installing and uninstalling Terminal Services Licensing
- Activating Terminal Services Licensing
- Deactivating Terminal Services Licensing
- Viewing Help for Terminal Services and Terminal Services Licensing

To install or uninstall Terminal Services Licensing

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. In Windows Components, select **Terminal Services Licensing**, and do one of the following:
   - If Terminal Services Licensing is installed and you want to remove it, clear the check box for Terminal Services Licensing and complete the Licensing Wizard.
   - If Terminal Services Licensing is not installed and you want to add it, select the check box for Terminal Services Licensing and then click **Next**.
5. In Terminal Services Licensing Setup, do one of the following:
   - If your network includes several domains, click **Your entire enterprise**, and then provide the database location. An enterprise license server can serve Terminal servers on any Windows 2000 domain.
   - If you want to maintain a separate license server for each domain, or if your network includes workgroups or Windows NT 4.0 domains, click **Your domain or workgroup**, and then provide the database location.

To activate a license server

As mentioned previously in this section, you must activate a Terminal Services license server before it can issue licenses to Terminal Server clients. Use Terminal Server Licensing to activate a Terminal Services license server through the Microsoft Clearinghouse.

You can find procedure checklists along with complete instructions for configuring and activating Terminal Services license servers in Windows 2000 Server Help. Search for Terminal Services Licensing in the Windows Help Index. To view Help see the procedure below titled "To view Help for Terminal Services and Terminal Services Licensing."

To deactivate a license server

If Terminal Services and Terminal Services Licensing are already installed and you want to deactivate the license server, use the following procedure. You might need to deactivate a license server when the certificate of the server has expired, when the server becomes corrupted, or when the server is being redeployed. Note that when a license server's registration has expired, you are prompted to reactive the license server (not deactivate it). When you deactivate a license server, you will not be able to license additional clients from this server until the license server is reactivated.

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Terminal Services Licensing**.
2. In the console tree, right-click the license server you want to deactivate, point to **Advanced**, and then click **Deactivate Server**. The Licensing Wizard starts.
3. In Information Needed, confirm that your name, phone number (optional), and e-mail address (required if you are using the Internet method) are correct, and then click **Next**.
4. Your request to deactivate the license server is sent to Microsoft where it is processed.

   Note The information sent to the Microsoft Clearinghouse during deactivation is the same information sent during activation, which includes company name, first and last name of the user, license server name, and license server ID.

5. Click **Finish**.

   Notes

   Deactivating a license server does not remove the component. As mentioned previously, follow the basic principle of stopping unnecessary services and keeping computers (especially servers) free from unnecessary software by removing the Terminal Services Licensing component if you no longer plan to use it as a license server.

   You cannot deactivate a license server using either the fax or Internet connection methods.

   When deactivating a license server by phone, you will receive a confirmation code from the Customer Support representative that must be typed in the appropriate space in the Licensing Wizard.

To view Help for Terminal Services and Terminal Services Licensing

1. Click **Start** and then click **Help**.

2. Click **Client Services** and then click **Terminal Services**.
3. To access information specific to Terminal Services Licensing, follow the previous steps and then:
4. Click **Managing Terminal Services** and then click **Licensing Terminal Services**.
5. To get information about the following procedures click **How To**:
    - Enable Terminal Services Licensing
    - Activate a license server
    - Install client license key packs
    - Deactivate a license server
    - Reactivate a license server
    - Repeat the installation of a client license key pack
    - Connect to a license server
    - Change the Licensing Wizard properties

Web Help

This section provides information about:

- The benefits of the Web Help feature in Help for Windows 2000
- Using Web Help in a managed environment

Benefits and purposes of Web Help

Web Help in Microsoft Windows 2000 Service Pack 3 (SP3) gives users direct access to many important resources on the Microsoft Web site. These resources include product support, Resource Kits, and information about compatible hardware and software. The Web Help feature can be accessed in a number of ways, including:

- Selecting Help\Web Help from the Start menu.
- Selecting Help\Web Help in Control Panel, My Network Places, My Computer, or My Documents.

When the user clicks the Web Help icon, an "Online support and information" list appears in the details pane of the Web Help window. The list contains the following links:

- Windows 2000 home page
- Get tips and practical advice about Windows 2000
- Contact product support
- Download updates, new features, and drivers from Windows Update
- Search for Windows 2000-compatible software
- Search for Windows 2000-compatible hardware
- Learn to deploy Windows 2000
- View Windows 2000 Resource Kit information
- Learn more about accessibility resources

These links direct the user to the appropriate Microsoft Web page where they can search for information or continue to navigate through the rest of the Microsoft Web site or access the Internet.

Using Web Help in a managed environment

Web Help is a default component of Windows 2000 and cannot be disabled. In a managed environment, however, it is unlikely that users will be allowed unfettered access to the Internet; this would normally be controlled by the IT department through configured settings on a firewall or proxy server.

Web Help can only access the Microsoft Web site when there is Internet connectivity; users are neither required nor prompted to connect to the Internet. When users select one of the options from the "Online support and information" list, they are taken to the appropriate Web page. From there the user has access to other pages and sites within Microsoft and through MSN.com to the Internet.

The links available through Web Help use HTTP protocol over port 80 to communicate. Web Help does not log or encrypt data. Because it is a default component it can not be disabled; therefore, the only method available to you for controlling Web Help is to restrict access to the Internet through firewall or proxy server settings.

You can configure your firewall to restrict access to the Internet through HTTP port 80. When traffic through HTTP port 80 is blocked in this way, Help searches will only query local Help content.

Related documentation

For more information about firewall design, policy, and security considerations for firewall design in general, you can consult the following reference:

Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly & Associates, Inc., 1995.

Windows Media Player

This section provides information about:

- The benefits of Microsoft Windows Media Player
- How Windows Media Player communicates with sites on the Internet
- How to control Windows Media Player to limit the flow of information to and from the Internet

Notes

The version of Windows Media Player that comes with Windows 2000 (version 6.4) is no longer supported. We therefore recommend that you install Windows Media Player 9 Series, which is the version described in this section, and which can be downloaded for use with Microsoft Windows 2000 Service Pack 3 (SP3).

Depending on the intended use of the client, we recommend that you take one of the following two approaches to installing and configuring Windows Media Player:

- **On a client used for viewing streaming media**: If the client will be used for viewing streaming media (for example, music and videos), we recommend you upgrade to Windows Media Player 9 Series on that client and on all servers from which you want to control that client. Completing these upgrades makes it easier to control Windows Media Player at an administrative level, and therefore makes it easier to limit the ways that users can initiate communication with Internet sites through Windows Media Player.
- **On a client not used for viewing streaming media**: If the client will not be used for viewing streaming media, remove the visible entry points to Windows Media Player on that client, and as an additional option, use Group Policy to prevent the user from running the Windows Media Player executable, Wmplayer.exe. These methods help prevent users from starting Windows Media Player and from initiating communication with Internet sites through Windows Media Player.

For more information about Windows Media Player 9 Series, see the following Microsoft Web site:

www.microsoft.com/windows/windowsmedia/

Benefits and purposes of Windows Media Player

Microsoft Windows Media Player (also called the Player) enables users to play and organize digital media files on their computer and on the Internet. Users can play CDs and DVDs (if they have DVD hardware), create custom CDs, listen to radio stations, search for and organize digital media files, and copy files to a portable device.

The latest version of Windows Media Player available for downloading to Windows 2000 SP3 enables you as the administrator to configure the Player to control access to certain consumer features. The management and deployment features enable you to bring customized media functionality to your organization's employees to enhance productivity.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization where users connect to sites on the Internet or download items from the Internet. This section, however, provides information about Windows Media Player that can help you balance your organization's requirements for communication across the Internet with your organization's requirements for protection of networked assets.

For more information about deploying and managing Windows Media Player in an enterprise environment, see the Windows Media Web site at:

www.microsoft.com/windows/windowsmedia/

Overview: Using Windows Media Player in a managed environment

The Windows Media Player version that comes with Windows 2000 (version 6.4) is an integral component of the operating system and is installed by default. Because it offers fewer configuration options, however, we recommend that you install Windows Media Player 9 Series on both your client and server to take advantage of the advanced control features and Group Policy settings available in the newer version. With the newer version you can use an answer file to hide entry points to the user interface. You can also customize the Player to make certain aspects of it either available, of limited use, or unavailable to the user in accordance with policies in your organization.

There are a variety of options available to you when considering how you want your users to interact with Windows Media Player. To help you assess what level of control to apply to your organization, the following table summarizes the configuration options available for various control requirements.

Options for controlling communication with the Internet through Windows Media Player

Options	Degree of control
Limit users ability to see Windows Media Player icons and start Wmplayer.exe. For more information about hiding the entry points during unattended installation, see "Procedures for configuration of Windows Media Player" later in this section.	Least access to the Internet and to media content, but least flexible. With this option users are prevented from accessing the Player from any of the usual entry points.
Allow users to have Windows Media Player available but with access only to the organization's intranet media server. For more information, see Help for servers running Windows 2000, specifically, the Help that is installed when you install the Windows Media Services component.	Strongly restricted access to the Internet, but requires investment in time and money to implement an internal media server. With this option users have access to the Player but can only play content that is available on a media server on an organization's intranet. The user has no access to the Internet.
Allow users to have Windows Media Player available with access to only those Internet sites that are approved for access by an organization's policies. Use an inclusion list (through the firewall or proxy or both).	Restricted access to Internet, but requires knowledge of which external sites are trustworthy.
Allow only certain users to have access to the	Restricted access to some users, but access to

Internet. All others are restricted by various means.	Internet available only to users who need it most. Implies that training is provided to selected users who are held accountable.
Allow users to have Windows Media Player available but with access to only certain features. Use Group Policy settings (on a server) to configure Windows Media Player on clients. For more information, see "Controlling Windows Media Player to limit the flow of information to and from the Internet" and "Procedures for configuration of Windows Media Player" later in this section.	Moderate control and moderate flexibility. With this option the user has access to the Player but you maintain control over which options they are able to use.
Free access for all.	Highest access to the Internet and media content.

The following subsections describe how the Windows Media Player 9 Series communicates with the Internet and how to control the flow of information to and from the Internet. It also gives procedures for using Group Policy to control the user interface, playback, networking, and updates for Windows Media Player.

How Windows Media Player communicates with sites on the Internet

The Windows Media Player interface opens locally when the user navigates through the Start/Programs menu or clicks the shortcut on the desktop. When the user selects either Media Guide, Radio Tuner, Premium Services, or Skin Chooser/More Skins from the Player taskbar, Windows Media Player connects to www.WindowsMedia.com through either a local area network (LAN) or a modem connection.

Communication with the WindowsMedia.com site

When connection is made with the Internet, WindowsMedia.com provides the following key features:

- Metadata retrieval
- Metadata submission
- Media guide
- Radio tuner
- Premium services
- Codec download
- Player update
- Newsletter signup
- Downloadable skins
- Downloadable visualizations
- Downloadable plug-ins

- Downloadable device service providers (SPs)
- Customer experience improvement program
- Windows Media digital rights management (DRM) Internet access

Communication with other sites

WindowsMedia.com is a Web site operated by Microsoft and is tightly integrated into Windows Media Player. Media Guide and Radio Tuner are Web pages provided by WindowsMedia.com. All the CD audio data, DVD data, radio presets, and the information in the Info Center View pane of the Now Playing feature also come directly from WindowsMedia.com. Other services provided by WindowsMedia.com include the Player updates and download support for codecs, skins, and visualizations. (A codec, short for compressor/decompressor, is software that compresses or decompresses audio or video data.)

To support the playback of secure content, Windows Media Player will also contact:

- Non-Microsoft DRM license servers
- Microsoft DRM upgrade service

Data exchanged during connection with the Internet

The other common Internet connections that Windows Media Player makes are to media servers run by content providers.

Data exchanged during communication

The following list describes various aspects of the data that is sent to and from the Internet through Windows Media Player, and how the exchange of information takes place:

- **Specific information sent or received**: The key features of WindowsMedia.com listed previously communicate information between the Internet and the user's computer as follows:
    - **Non-Microsoft digital rights management (DRM) license servers.** The license servers enable users to acquire licenses to play back content protected with Microsoft DRM technology. The license acquisition process updates the user's DRM revocation and exclusion lists. These lists are used to block compromised applications from accessing secure content.
    - **Microsoft DRM upgrade service.** The upgrade service provides users with the option to upgrade their DRM components should the secure content they want to play require upgraded components (for example, an individualized black box).
    - **Media servers run by content providers.** To provide streaming media, it is necessary for Windows Media Player to communicate directly with a media server. These servers are typically operated by non-Microsoft content providers, and are not under Microsoft control.
    - **Metadata retrieval.** When the user triggers a metadata request (see the bulleted item, "User notification and triggers"), a CD table of contents or DVD identification is sent from the user's computer, and then metadata is retrieved. The metadata can include album art, track names, lyrics, and even artist bios. It is stored in the user's media library for offline use.

- **Metadata submission.** This is a service that enables users to submit corrections to the WindowsMedia.com metadata database. A cookie (if not blocked), CD table of contents or DVD identification, and user's corrected metadata are sent.
- **Media guide.** Media Guide is a set of Web pages, hosted within the Windows Media Player interface, that focuses on streaming media. A cookie is sent up (if not blocked); the Media Guide Web page from WindowsMedia.com is returned.
- **Radio tuner.** Radio Tuner is a set of Web pages, hosted with the Windows Media Player interface, that focuses on Internet radio stations. A cookie is sent up (if not blocked); the Radio Tuner Web page is returned, with pre-sets (if the cookie is not blocked).
- **Premium services.** Premium Services is a set of Web pages, hosted within the Windows Media Player interface, that enables users to visit and subscribe to premium content service providers. A cookie is sent up (if not blocked); the Premium Services Web page returns media content that can be played in the Player.
- **Codec download.** This service enables users to acquire certain codecs during playback if they are not resident on the user's system. A cookie (if not blocked) and codec are sent up; a codec is returned and installed if available.
- **Player update.** This service enables users to detect and acquire updated Windows Media Player components. A cookie (if not blocked) and a version number of Windows Media Player components are sent; components are returned and installed if available and the user has given consent. The automatic check and manual update options are only available to users with administrative credentials.
- **Newsletter signup.** The Media Guide provides a link to the Microsoft Network (MSN) newsletter service that enables users to sign up for the WindowsMedia.com newsletter. An MSN cookie (if not blocked) and the user's e-mail address are sent directly to the MSN newsletter service.
- **Downloadable skins.** Additional Skins is a Web page that contains extra downloadable skins. A cookie is sent up (if not blocked); the Downloadable Skins Web page is returned in the Microsoft Internet Explorer browser.
- **Downloadable visualizations.** Additional Visualizations is a Web page that contains extra downloadable visualizations. A cookie is sent up (if not blocked); the Downloadable Visualizations Web page is returned in the Internet Explorer browser.
- **Media library.** The Media Library lists the user's collection of audio and video files, as well as links to sources for audio and video. This information can be accessed by other software on the user's computer and on the Internet.
- **Downloadable plug-ins.** Downloadable Plug-ins is a Web page that contains new features that can be added to Windows Media Player. A cookie is sent up (if not blocked); the Plug-ins Web page is returned in the Internet Explorer browser.
- **Downloadable device SPs.** Downloadable Device service providers (SPs) provide a link to the Cool Devices Web page. This Web page offers users information about a variety of portable media devices, and it gives them the option of purchasing these devices online. Users can also download media drivers for those devices. A cookie is sent up (if not blocked); the Cool Devices Web page is returned in the Internet Explorer browser.
- **Customer experience improvement program.** This option, which is available through the Tools\Options\Privacy tab, specifies whether to send anonymous Windows Media Player usage information to Microsoft. The anonymous information obtained from the user is used to improve the Player and related services.

- **Cookies**. Windows Media Player uses the Internet as a networking and information source. When accessing the Internet, cookies may be downloaded to the user's computer or uploaded to a media service.
- **Site logs**. There are two types of logs created as follows:
  - **Raw IIS log**. A standard Internet Information Services (IIS) log that records all requests to the server. This log includes the IP address of the client and a cookie. It is not encrypted.
  - **Tracking log**. This log contains all requests. It includes the IP address of the client and a cookie. It is neither encrypted nor correlated with personally identifiable information. The Player also generates a streaming media log and sends it to any media servers that exist on your network.

- **Default and recommended settings**: Some of the Windows Media Player features and options are enabled by default. Such options as the globally unique identifier (GUID) that uniquely identifies the Player, and metadata downloaded for files are not enabled. Recommended settings are described in the next subsection, "Controlling Windows Media Player to limit the flow of information to and from the Internet."
- **Trigger and user notification**: The WindowsMedia.com features are triggered individually by various user interactions as listed below. The user may or may not be notified at that time depending on the feature being triggered.
  - **Metadata retrieval.**
    - **Notification.** The user is not notified.
    - **Trigger.** When the user first inserts a CD or DVD, or when the user requests detailed information, (for example, by using the Media Details button), information is retrieved automatically from WindowsMedia.com.
  - **Metadata submission.**
    - **Notification**. The user is notified.
    - **Trigger.** When the user submits corrected metadata for files, CDs, and DVDs, information is sent to WindowsMedia.com.
  - **Media guide.**
    - **Notification.** The user is not notified.
    - **Trigger.** The media guide is triggered automatically if the user selects the **Start Player in Media Guide** check box on the Player tab in the Options dialog box, or when the user selects **Media Guide** from the taskbar.
  - **Radio tuner.**
    - **Notification**. The user is not notified.
    - **Trigger.** When the user selects **Radio Tuner** from the taskbar the Radio Station Selection Web page is triggered.
  - **Premium services.**
    - **Notification.** The user is not notified.
    - **Trigger.** When the user selects **Premium Services** from the taskbar the Premium Services Web page is triggered.

- **Codec download.**
  - **Notification.** There is no Windows Media Player pop-up message.
  - **Trigger.** A security dialog box will pop up if the site is not trusted. The Windows Media Player status bar will indicate that a codec is being downloaded.
- **Player update.**
  - **Notifications.** The user is notified. The user is prompted to download but can decline to do so.
  - **Trigger.** At a set frequency, if the user is online and is logged on as an administrator, a check is made for updated Windows Media Player components.
- **Newsletter signup.**
  - **Notification.** The user is notified, although the user does not have to subscribe to the newsletter.
  - **Trigger.** The trigger occurs when the user selects **Subscribe to our free newsletter** on the Media Guide.
- **Downloadable skins.**
  - **Notification.** The user sees the download progress dialog box after the selection is made.
  - **Trigger.** Users select **More skins** from the Skin Chooser menu, which brings up the Downloadable Skins Web page. When users select a skin from this screen, they are prompted to accept or reject the download. If they accept, the skin is downloaded.
- **Downloadable visualizations.**
  - **Notification.** The user sees the download progress dialog box after the selection is made.
  - **Trigger.** The user selects **Download Visualizations** from the Tools\Download\ Visualizations menu, which brings up the Downloadable Visualization Web page. When the user selects a visualization from this screen, they are prompted to accept or reject the download. If the user accepts, the visualization is downloaded.
- **Downloadable plug-ins.**
  - **Notification.** The user must specifically select to purchase and download a plug-in from a product-specific Web site. The user sees the download progress dialog box after the selection is made.
  - **Trigger.** Users select **Download Plug-ins** from the Tools\Download\Plug-ins menu or from the View\Plug-ins menu, or they select **Look for Plug-ins on the Internet** on the Tools\Options\Plug-ins tab, which brings up the Downloadable Plug-ins Web page. When users select a plug-in from this screen, they are prompted to accept or reject the download. If they accept, the plug-in is downloaded.
- **Downloadable device SPs.**
  - **Notification.** The user must specifically select to purchase and download a plug-in from a product-specific Web site. The user sees the download progress dialog box after the selection is made.
  - **Trigger.** Users select Tools\Download**Downloadable Device SPs**, or they select **Supported portable devices and drivers** from the Items on the Device drop-down

list in the Copy to CD or Device window. When the user purchases a portable device or driver the device or driver is downloaded.

- **Customer experience improvement program.**
  - **Notification.** The user is not notified when information is transferred.
  - **Trigger.** Users select the following check box on the Tools\Options\Privacy tab: **I want to help make Microsoft software and services even better by sending the Player usage data to Microsoft**. If they accept, Microsoft will collect anonymous information about their hardware configuration and how they use the software and services so that Microsoft can identify trends and usage patterns.
- **Media library.**
  - **Notification.** The user is not notified.
  - **Trigger.** The trigger occurs when the user adds purchased media to the library from WindowsMedia.com or another media vendor. Access can be turned off through the Media Library tab on the Tools\Options menu.
- **Cookies.**
  - **Notification.** The user is not notified.
  - **Trigger.** The trigger occurs automatically when a Web site is accessed. Cookie downloads can be blocked from the Privacy tab in the Options dialog box.

- **Logging**: Logging occurs when information is sent from the Player to a streaming media server or to an Internet Server Application Programming Interface (ISAPI) logging a dynamic-link library (DLL) running on Internet Information Services (IIS). For more information about logging and server performance issues, refer to the white paper titled, "Best Practices for Windows Media Technologies" at the following site:

  www.microsoft.com/technet/prodtechnol/netshow/plan/wmtbest.asp

  Logging informs the server of various pieces of information so that services can be improved. The information includes such details as connection time and the Internet protocol (IP) address of the computer that is connected to the server (typically a Network Address Translation [NAT] or proxy server). It also includes the version, identification number (ID), date, and protocol of Windows Media Player. Most information is neither unique nor traceable to the user's computer. For more detailed information about the exchange of information in Windows Media Player, see the bulleted item, "Privacy policy."

- **Encryption**: Windows audio media can be encrypted using the Secure Audio Path feature in Digital Rights Management (DRM). The Secure Audio Path feature maintains audio encryption beyond the Player application. It is a feature of Microsoft Windows that maintains the security and protection of digital music that has been encrypted by using DRM technology. Secure Audio Path provides an infrastructure for maintaining copy protection on music. The client can progressively download content from a Web server using HTTPS. A client and server may also use Internet Protocol security (IPSec) to encrypt packets that traverse the network.

- **Uniquely identify user**: Windows Media Player at no time requests any personally identifiable information (such as name, address, or phone number).

- **Privacy policy**: Windows Media Player and WindowsMedia.com both have published privacy statements that detail their data collection and use practices. These documents are available to users at the following locations:
  - The Windows Media Player privacy statement at:

www.microsoft.com/windows/windowsmedia/privacy/9splayer.asp

- The WindowsMedia.com privacy statement at:

  windowsmedia.com/privacy/privacystatement.asp

- **Transmission protocol**: With Windows Media Player you can specify that selected protocols are used while receiving streaming media from a media server using either Microsoft Media Server (MMS) or Real-Time Streaming Protocol (RTSP) protocols as follows:

  Windows Media Player interprets the media stream coming from the media server and tries User Datagram Protocol (UDP). If the stream is from a server running Windows Media Player 9 Series, the Player will try RTSP/UDP. If the media stream is coming from server running a previous version of the Player, the Player will try MMS/UDP. If the Player is unable to connect through UDP (for example, if it is behind a firewall that doesn't allow UDP), the Player tries the Transmission Control Protocol (TCP), and then it tries HTTP if it can't make a connection with TCP on the desired port. This protocol rollover takes place by moving from the most efficient protocol (UDP) to the least efficient protocol (HTTP), because not all firewalls have the necessary ports open to play Windows Media streams.

  - **Multicast**. Routers will not pass multicast streams across an intranet unless specifically configured to do so.
  - **UDP**. UDP is used with port selection if required due to firewall or proxy issues. If the UDP check box is selected and the UDP ports box is blank, the Player uses default ports when playing content from an MMS URL. If the UDP check box is not selected, the information in the UDP ports box is ignored. If using a network address translation (NAT), UDP will fail unless the NAT supports dynamic opening of ports through Universal Plug and Play.
  - **TCP.** TCP means either MMS over TCP or RTSP over TCP.
  - **HTTP**. When the HTTP protocol is selected, the HTTP protocol is used to receive streaming media from an MMS or RTSP URL.

  If none of the protocols is selected, content from an MMS or RTSP URL cannot be played.

- **Port**: The Windows Media Player client communicates across random ports as designated by the operating system. The server port is a "well-known port" as follows:

  - **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.
  - **Real Time Streaming Protocol (RTSP) UDP or TCP**: The port number is 554.
  - **Microsoft Media Server (MMS) UDP or TCP**: The port number is 1755.

  In a TCP connection there is only one socket created. (A socket is an identifier for a particular service on a particular node on a network.) You therefore need only one port number on the client and one on the server. Commands (such as play, pause, and fast forward) and data (audio and video) are sent across the same socket connection. In UDP connections, however, the client makes a TCP connection to the server and sends commands over it. The server then opens a UDP socket to the client. It is over this second socket that the audio and video data is sent. And it is this second socket that firewalls and proxies typically block.

  In an HTTP streaming connection using HTTP/1.0, there is only one socket opened at a time. (The version of HTTP in use before July 1999 was HTTP/1.0, and the version in use since then is HTTP/1.1.) With HTTP/1.0, for each play, pause, stop, fast forward, or rewind operation the original socket is closed, another socket is opened, and this second socket will more than likely use a different port number on the client. (There are other operations that use more than one socket.)

If the enterprise network implements a firewall that prevents users from receiving streams that use the UDP or TCP protocols, Windows Media Player can be configured to work with firewalls as described in the next bulleted item.

- **Windows Media and firewalls:** Windows Media normally streams through UDP/IP on a wide range of ports (these port numbers are provided later in this list). Aware of the possible security issues that a range this size can cause, Microsoft has also enabled Windows Media to stream with TCP/IP through port 1755 or with RTSP through port 554. For those sites where opening a port that is not "well-known" is a problem, Windows Media can also stream through HTTP on port 80. (HTTP streaming from Windows Media Services is disabled by default.) Some firewalls have a preconfigured NetShow Player setting (the former name for Windows Media Technologies), which may work for Windows Media.

  - **Firewall settings for Windows Media**
    There are five primary scenarios to consider when you set up a firewall to accommodate Windows Media:

    - Using Windows Media Player behind a firewall to access content outside the firewall
    - Using Windows Media Player outside a firewall to access content on a media server behind a firewall
    - Using Windows Media Encoder outside a firewall to communicate with a media server behind the firewall, or to communicate between two servers across a firewall
    - Using Windows Media Administrator outside a firewall to manage a media server behind a firewall
    - IP multicast

    This section of the white paper describes only the first and last scenarios, that is, the client behind the firewall and IP multicast. In the examples below, the in port is the port that the server uses to get past the firewall. The out port is the port that Microsoft Windows Media Player or other clients use to communicate with the server. The port assignment is random between 1024 and 5000.

    - **Client configuration behind a firewall**
      A firewall configuration that enables users with Windows Media Player behind a firewall to access media servers outside the firewall is as follows:

      Streaming ASF with UDP
      Out: TCP on port 1755
      Out: UDP on port 1755
      In: UDP between ports 1024 and 5000 (As a security measure, estimate the number of ports you will need by determining how many clients you expect, and open only that number of ports.)
      In: RTSP on port 554

      Streaming ASF with TCP
      In and out: TCP on port 1755
      In and out: RTSP on port 554

      Streaming ASF with HTTP
      In and out: TCP on port 80

    - **IP multicast**
      Choosing to allow Windows Media streaming through IP multicast is simply a choice to allow traffic that is addressed to the standard Class D IP addresses (224.0.0.0 through 239.255.255.255). As of this writing, most routers have IP multicast disabled;

router companies made a decision to have their equipment default to disable IP multicast at a time when a typical video stream took up 30 percent of a 10BaseT network. (10BaseT is the Ethernet standard for baseband local area networks.)

Microsoft is working with major router vendors to reverse this situation, now that media streams are compressed and standards are in place that eliminate unwanted multicast traffic. The Internet Group Management Protocol (IGMP) supported by Windows Media assures that multicast traffic passes through the network only when a client has requested it. Windows Media streams are highly compressed, usually only taking up the bandwidth of a single modem connection.

The following firewall configuration enables IP multicasting:

Streaming ASF with multicast
IP multicast address range: 224.0.0.1 through 239.255.255.255
To enable IP multicasting you must allow packets sent to this standard IP multicast address range to come through the firewall. This IP multicast address range must be enabled on both client and server sides, as well as on every router in between.

For more information about firewall settings for Windows Media, search for the latest information on the Windows Media Web site at:

www.microsoft.com/windows/windowsmedia/

Information about firewall settings can also be found on the Windows Media Web site at:

www.microsoft.com/windows/windowsmedia/serve/firewall.aspx

- **Ability to disable**: All key features are enabled by default; however, each can be disabled through the Tools\Options menu in Windows Media Player, through the use of Group Policy, or through an answer file during unattended installation. For more information, see "Settings that can be controlled through Group Policy" and "Procedures for configuration of Windows Media Player" later in this section.

Controlling Windows Media Player to limit the flow of information to and from the Internet

As mentioned previously, if Windows Media Player is widely used in your organization, we recommended that you upgrade to the latest version, Windows Media Player 9 Series, after installing Windows 2000 SP3. If the Player is not widely used in your organization, you can remove all visible entry points to it by using the procedure described in the subsections that follow.

The most effective method of eliminating access to Windows Media Player is to remove entry points to the Player during unattended installation. If Windows Media Player is being used in your organization, however, you can control individual features of the Player either through the Tools\Options menu or through Group Policy. The recommended method for controlling the features in a managed environment is through Group Policy. The following lists describe options for controlling Windows Media Player by using Group Policy and through other methods. For details about configuring these options, see "Procedures for configuration of Windows Media Player" later in this section.

Settings that can be controlled through the user interface in Windows Media Player

You can control the following through the user interface in Windows Media Player:

- **Metadata retrieval.** Do not insert the CD or DVD. Clear the **Update my music files by retrieving missing media information from the Internet** check box on the Media Library and Privacy tabs. Clear the **Retrieve media information for CDs and DVDs from the Internet** check box on the Privacy tab.
- **Metadata submission.** Do not submit metadata.
- **Media guide.** Clear the **Start Player in Media Guide** check box on the Player tab.
- **Radio tuner.** Use a custom skin with no Radio Tuner access.
- **Codec download.** Clear or check the **Download Codecs Automatically** check box on the Player tab.
- **Newsletter signup.** Use a custom skin; eliminating access to Media Guide eliminates access to the newsletter signup.
- **Downloadable skins.** Use a custom skin that does not display downloadable skins.
- **Downloadable visualizations.** Use a custom skin that does not display downloadable visualizations.
- **Download plug-ins**. Do not select the **Download Plug-ins** options from any of the trigger locations mentioned previously.
- **Download Device SPs**. Do not select the **Download Device SPs** options from any of the trigger locations mentioned previously.
- **Customer experience improvement program**. Enable the **Hide Privacy Tab** Group Policy setting to keep users from changing this option in that tab. Enable the **Do Not Show First Use Dialog Boxes** Group Policy setting to keep users from changing this option in those dialog boxes.
- **Connect to the Internet.** Do not select the **Connect to the Internet** check box on the Player tab.
- **Licenses.** Clear the **Acquire licenses automatically for protected content** check box on the Privacy tab.

Settings that can be controlled through Group Policy

The following configuration settings for Windows Media Player can be controlled through Group Policy. To access the Windows Media Player 9 Series Group Policy settings, this version must be installed on both the server and the client. For a procedure for locating the Group Policy settings for configuring Windows Media Player, see "Procedures for configuration of Windows Media Player" later in this section.

- **Prevent CD and DVD Media Information Retrieval**

  This policy setting prevents the Player from automatically obtaining media information from the Internet for CDs and DVDs. This policy setting also ensures that this function is not available through the Privacy tab in the Options menu of the Player and First Use dialog box during installation.

- **Prevent Music File Media Information Retrieval**

  This policy setting prevents the Player from automatically obtaining media information for music files from the Internet. This policy setting also ensures that this function is not available

through the Privacy and Media Library tabs in the Options menu of the Player and First Use dialog box during installation.

- **User interface settings**
  - **Hide Privacy tab**

    When you hide this tab, users cannot configure privacy settings for Windows Media Player.
  - **Hide Security tab**

    When you hide this tab, users cannot configure security settings for Windows Media Player.
  - **Set and lock skin**

    You can use a custom skin that eliminates access to functionality you want to control, specifically, Radio Tuner, Media Guide, display of downloadable skins, or display of downloadable visualizations.
  - **Do Not Show Anchor**
- **Playback setting**
  - **Prevent Codec Download**
- **Networking settings**
  - **Hide Network tab**

    When you hide this tab, users cannot configure network settings for Windows Media Player.
  - **Streaming Media Protocols**

    The protocols to choose from are Multicast, UDP (enter UDP ports if required), TCP, and HTTP, as described in "How Windows Media Player communicates with sites on the Internet" earlier in this section.
  - **Configure HTTP Proxy**

    This Group Policy setting is ignored if the setting for **Streaming Media Protocols** is enabled and HTTP is not selected. When this Group Policy setting is disabled, the Player cannot use the HTTP proxy and the user cannot change the HTTP proxy settings on the Network tab in Windows Media Player.
  - **Configure MMS Proxy**

    This Group Policy setting is ignored if the setting for **Streaming Media Protocols** is enabled and multicast is not selected. When this policy setting is disabled, the Microsoft Media Server (MMS) proxy cannot be used and the user cannot change the MMS proxy settings on the Network tab in Windows Media Player.
  - **Configure RTSP Proxy**

    When this Group Policy setting is disabled, the RTSP proxy server cannot be used and users cannot change the RTSP proxy settings on the Network tab in Windows Media Player.
  - **Configure Network Buffering**
  - **Player Update**

There is no Group Policy setting specific to Windows Media Player for this option. You can, however, control the Player updates by enabling **Remove access to use all Windows Update features** in the Windows Update folder or disabling **Windows Automatic Updates** in the System folder.

Other ways to control Windows Media Player

You can control several aspects of Windows Media Player through means other than the user interface or the individual Group Policy settings. Other methods for controlling the Player include:

- Preventing users from starting Windows Media Player through Group Policy by adding Wmplayer.exe to a list of Windows applications that cannot be run. For more information, see "To prevent users from starting Windows Media Player by using Group Policy" later in this section. This will prevent users from opening the Player by double-clicking media files or through other indirect methods.
- Using the firewall or proxy or both to block access to the WindowsMedia.com Web site.
- Creating custom player skins that contain only those features that you want users to use. For information about creating custom skins you can refer to the following sites:

  msdn.microsoft.com/library/default.asp?url=/library/en-us/wmplay/mmp_sdk/windowsmediaplayerskins.asp

  msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwmt/html/WMPlayer_9_SDK_Intro.asp

Procedures for configuration of Windows Media Player

Windows Media Player can be configured in several ways as described previously. This subsection provides procedures for:

- Locating Group Policy settings for configuring Windows Media Player
- Preventing users from starting Windows Media Player by using Group Policy
- Accessing the Network tab on the user interface in Windows Media Player (to set streaming media protocols)
- Disabling the update feature in Windows Media Player for Windows 2000 using Group Policy
- Removing visible entry points to Windows Media Player during unattended installation by using an answer file

Important To prevent users from manually updating Windows Media Player, we recommend that those users are not set up with administrative credentials on their computers.

To locate Group Policy settings for configuring Windows Media Player

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."

2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Media Player**.
3. View the Group Policy settings that are available. For more information about these settings, see the list under "Settings that can be controlled through Group Policy" earlier in this section.

To prevent users from starting Windows Media Player by using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
3. In the details pane, double-click **Don't run specified Windows applications**.
4. Select **Enabled**, click **Show**, click **Add**, and then enter the application executable name, Wmplayer.exe.

Setting streaming media protocols

There are two methods for setting streaming media protocols. One method, described in the following procedure, is to use the Network tab to both configure the protocols and proxy settings that you want Windows Media Player to use when receiving streaming media files, and to then hide the Network tab through the use of Group Policy in Windows Media Player. The second method is to use Group Policy directly. For more information about using Group Policy, see "To locate Group Policy settings for configuring Windows Media Player" and "Settings that can be controlled through Group Policy" earlier in this section.

To access the Network tab on the user interface in Windows Media Player

1. On the **Tools** menu, click **Options**, and then click **Network**.
2. The following options are listed on the Network tab:
   - **Protocols.** Specifies the protocols that Windows Media Player can use to receive a stream. Select one or more of the following:
     - Multicast
     - UDP
     - TCP
     - HTTP

     By default, all protocols are selected, which means that the Player attempts to use each protocol to receive a stream. Because the Player can receive files using a variety of protocols, we recommend that you select all protocols.
   - **Use ports.** Specifies a particular port or port range, if UDP is the protocol used to receive streaming content. This option is useful if your network or firewall administrator has established a specific port that enables streaming content to pass through. Unless otherwise instructed, Windows Media streams attempt to pass through firewalls on port 1755.

- **Proxy settings**. Select one of the following:
  - HTTP
  - MMS
  - RTSP

  Proxy settings specify how each protocol operates with a proxy server. Proxy servers are used when networks are protected by firewalls. If your network is behind a firewall, and you do not know how to configure your settings, please refer to the "Windows Media and Firewalls" item in the list under "How Windows Media Player communicates with sites on the Internet."
- **Configure button.** Click this button to change the proxy settings of the selected protocol. The following table lists the options for configuring a protocol to work with a proxy server.

Options for configuring a protocol to work with a proxy server

This option	Specifies that
Autodetect proxy settings	The Player discovers the ports that are open and uses them to receive streaming content.
Use proxy settings of the Web browser	The Player uses the same HTTP configuration as your browser to access network communication.
Do not use a proxy server	The Player does not attempt to communicate with a proxy server. Typically, this means that the Player does not receive streaming content from the Internet.
Use the following proxy server	The Player uses the proxy server and port you specify. Select **Bypass proxy server for local addresses** if you do not want the Player to use the proxy server when streams are from local servers.

Disabling the update feature in Windows Media Player for Windows 2000 using Group Policy

Windows Media Player for Windows 2000 does not have a Group Policy setting to disable the check for update features, however, there is another option that can be used to disable the automatic updates feature. This option is to enable **Remove access to use all Windows Update features** in the Windows Update folder or to disable **Windows Automatic Updates** in the System folder.

To disable the update feature in Windows Media Player for Windows 2000 through Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, and then click **Windows Components**.
3. In the details pane, double-click **Remove access to use all Windows Update features**.
4. Select **Enabled**.

You can alternatively follow this procedure to achieve the same results.

1. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
2. In the details pane, double-click **Windows Automatic Updates**.
3. Select **Disabled**.

To remove visible entry points to Windows Media Player during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, include the following entry:

   WMPOCM = Off

Additional information about this procedure is as follows:

- You can use WMPOCM in an answer file only if you are using the integrated installation method for SP3, which enables you to simultaneously install Windows 2000 and the service pack. If you plan to install Windows 2000 by itself and then later apply SP3, you cannot use WMPOCM in an answer file. For more information about the integrated installation methods for SP3, see the Service Pack 3 Installation and Deployment Guide at the following Web site:

  www.microsoft.com/windows2000/downloads/servicepacks/sp3/spdeploy.htm

- Omitting the WMPOCM entry from the answer file or using WMPOCM = On will cause Windows Media Player entry points to be visible after the Windows installation has been completed, which is the default behavior.
- This entry does not remove any Windows code, including any Windows Media Player code. Only the visible entry points for the Windows Media Player are removed.

Windows Media Services

This section provides information about:

- The benefits of Windows Media Services on servers running Microsoft Windows 2000 Service Pack 3 (SP3). (It is not included with Windows 2000 Professional.)
- For servers from which you want to offer content that will be streamed to an intranet or the Internet, the following types of information:
  - Examples of features in Windows Media Services 4.1 that help you control communication to and from a Windows Media server. Version 4.1 is the version of Windows Media Services included with the Windows 2000 Server family.
  - References to more detailed information about Windows Media Services, including information about ports and security-related topics.
  - Information about installing the Windows Media Services component, along with instructions for viewing the Help that comes with the component.
- For servers from which you do not want to offer content on an intranet or the Internet, information about excluding or removing Windows Media Services.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running servers that communicate across the Internet. This section, however, provides overview information as well as suggestions for other sources of information about balancing your organization's requirements for communication across the Internet with your organization's requirements for protection of networked assets.

Note This section of the white paper describes Windows Media Services (the server component), but it does not describe Windows Media Player (the client component) or Internet Information Services (IIS), both of which are involved in carrying out communication of multimedia content across the Internet. For information about these components, see the respective sections of this white paper.

Benefits and purposes of Windows Media Services

Windows Media Services is an optional component in products in the Windows 2000 Server family. With Windows Media Services, you can create, manage, and deliver Windows Media content over an intranet or the Internet. The clients receiving the content can render it as it is being received, that is, without downloading the content first. Streaming greatly reduces the wait time and storage requirements on the client. It also permits presentations of unlimited length, as well as live broadcasts.

The version of the Windows Media Services component included in the Windows 2000 Server family with SP3 is Windows Media Services 4.1.

For more information about features in Windows Media Services, see the sources in "Resources for learning about Windows Media Services" later in this section.

Examples of features that help you control communication to and from a Windows Media server

This subsection provides brief descriptions of some features in Windows Media Services 4.1 that help you control communication to and from a Windows Media server. These features are integrated with two aspects of basic functionality built into the Windows 2000 operating system:

- Authentication
- Controlling access by setting permissions

Authentication for Windows Media Services

Windows Media server components can be configured to require clients to be authenticated before they can access Windows Media unicast content. Authentication is not enabled by default when the Windows Media Services component is installed; however, you can enable one of the three authentication packages installed with Windows Media Services. When choosing a type of authentication, study the options available and compare them to your organization's requirements. The authentication options are as follows:

- **Windows NTLM authentication**: This method authenticates users who have accounts in Active Directory in a specific domain in Windows 2000. This form of authentication is best used on an intranet, where all users are part of the same or trusted domain.
- **HTTP-BASIC authentication and NTLM**. This method provides a standard way to validate HTTP users by using encoded plaintext passwords and user names. To play Advanced Streaming Format (ASF) content from a publishing point, the client must supply a user name and password. This method is available for use on the Internet or for intranet environments that require cross-platform authentication.
- **HTTP-BASIC authentication of accounts maintained through Commerce Server 2002**. This method provides a standard way to validate HTTP users by using encoded plaintext passwords and user names, and it checks client credentials against user accounts maintained in Microsoft Commerce Server 2002. This form of authentication is best for intranets that are not based on Windows domains, or for large-scale Internet or intranet implementations.

Authentication can be extended through the Windows Media Services Software Development Kit (SDK) to work with any user database that is compliant with ODBC (Open Database Connectivity) standards.

For more information about authentication in Windows Media Services or about the Windows Media Services SDK, see the list in "Resources for learning about Windows Media Services" later in this section.

Controlling access to content by setting permissions

With Windows Media Services in Windows 2000 Server with SP3, you can control access to content by setting permissions (also known as access control lists or ACLs) on a directory or a file (with the file extensions .asf, .wma, or .wmv). You can set permissions on individual files (or on whole directories) if you use NTFS as the file system on the partition where the files are stored. You can control access to on-demand content stored on a file allocation table (FAT) partition by setting permissions on the registry key associated with the on-demand unicast publishing point.

Note that if the source of a broadcast unicast publishing point is a live stream, the content is never stored on a physical storage device. If a file is not stored, you cannot assign permissions to it. To restrict access to a broadcast unicast stream, you must use Registry Editor to set permissions on the registry key associated with the broadcast unicast publishing point. You can also restrict access to Windows Media stations by setting permissions on the .nsc file (the file that describes a station to Windows Media Player) that is stored on a Web server.

To control access to content by setting permissions, you must also configure appropriate user accounts and enable one of the authentication packages installed with Windows Media Services.

In addition to the previous options, you can control client and server connections to Windows Media server components based on the IP address of the client or server attempting to connect.

Procedures for installing, removing, or excluding the Windows Media Services component

The following procedures explain how to:

- Include or exclude the Windows Media Services component during setup of a product in the Windows 2000 Server family on an individual computer
- Add or remove the Windows Media Services component on a computer after setup is complete for a product in the Windows 2000 Server family
- View the Help that comes with Windows Media Services
- Prevent the installation of Windows Media Services during unattended installation by using an answer file

To include or exclude Windows Media Services during Windows 2000 setup on an individual computer

1. During setup, when you see the Windows 2000 Components dialog box, scroll down to Windows Media Services.

   When Windows Media Services is selected, you can also click the **Details** button and view the check boxes for Windows Media Services subcomponents, and then click **Cancel** to return to the main components list.

2. If you want to include Windows Media Services, select the Windows Media Services check box, and if you want to exclude the component, clear the check box.
3. Continue with setup.

To add or remove the Windows Media Services component after setup is complete

1. Click **Start**, point to **Settings,** and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Select **Windows Media Services**.
5. Perform one of the following steps:

- If Windows Media Services is installed and you want to remove it, clear the check box for Windows Media Services and complete the wizard.
- If Windows Media Services is not installed and you want to add it, select the check box for Windows Media Services and complete the wizard.

If you want to view the list of Windows Media Services subcomponents, after selecting Windows Media Services, click **Details**.

To view the Help that comes with Windows Media Services

1. Make sure that the Windows Media Services component is installed by using one of the other procedures in this subsection.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Windows Media**.
3. Click **Product Documentation** (on the left).

To prevent the installation of Windows Media Services during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, include the following entry:

   WMS = Off

Resources for learning about Windows Media Services

The following list of resources can help you as you plan or modify your implementation of Windows Media Services and Windows Media Player in your organization:

- For conceptual and how-to information about using Windows Media Services, including information about authentication and permissions, see the Help that comes with the component. For information about installing the component and viewing Help, see "Procedures for installing, removing, or excluding the Windows Media Services component" earlier in this section.
- For selected information about ports and firewall or proxy settings, see the Windows Media Player section of this white paper.
- For more general information about ports and firewall or proxy settings, search for the latest information on the Windows Media Web site at:

  www.microsoft.com/windows/windowsmedia/

  Information about firewall settings can also be found on the Windows Media Web site at:

  www.microsoft.com/windows/windowsmedia/serve/firewall.aspx
- For information about deployment, including some information about firewall settings, see Windows Media Services Deployment Guide on the Microsoft Web site at:

  www.microsoft.com/windows/windowsmedia/serve/deployguides.aspx

- For information about best practices, including some information about firewall settings, see "Best Practices for Windows Media Technologies" on the TechNet Web site at:

  www.microsoft.com/technet/prodtechnol/netshow/plan/wmtbest.asp

- For documentation on the distribution of content, see the Windows Media Web site at:

  www.microsoft.com/windows/windowsmedia/distribute.aspx

- For information about Windows Media Services Software Development Kits (SDKs), see the Microsoft Developer Network Web site at:

  msdn.microsoft.com/downloads/list/winmedia.asp?frame=true

Windows Time Service

This section provides information about:

- The benefits of the Windows Time service
- How the Windows Time service communicates with sites on the Internet
- How to control the Windows Time service to limit the flow of information to and from the Internet
- How to monitor and troubleshoot the Windows Time service after configuration is complete

Benefits and purposes of the Windows Time service

Many components of Microsoft Windows 2000 Service Pack 3 (SP3) rely on accurate and synchronized time to function correctly. For example, without clocks that are synchronized to the correct time on all computers, Windows 2000 authentication might falsely interpret logon requests as intrusion attempts and consequently deny access to users.

With time synchronization, you can correlate events on different computers in an enterprise. With synchronized clocks on all of your computers, you ensure that you can correctly analyze events that happen in sequence on multiple computers. The Windows Time service automatically synchronizes a local computer’s time with other computers on a network to improve security and performance in your organization.

Overview: Using the Windows Time service in a managed environment

Computers keep the time on their internal clocks, which allows them to perform any function that requires the date or time. For scheduling purposes, however, the clocks must be set to the correct date and time, and they must be synchronized with the other clocks in the network. Without some other method in place, these clocks must be set manually.

With time synchronization, computers set their clocks automatically to match another computer's clock. One computer maintains very accurate time, and then all other computers set their clocks to match that computer. In this way, you can set accurate time on all computers.

The Windows Time service is installed by default on all computers running Windows 2000. The Windows Time service uses Coordinated Universal Time (UTC), which is independent of time zone. Time zone information is stored in the computer's registry and is added to the system time just before it is displayed to the user.

The Windows Time service starts automatically on computers that are joined to a domain. (For computers that are not joined to a domain, you can start the time service manually.) In a domain, time synchronization takes place when the Windows Time service turns on during system startup. In the default configuration, the Net Logon service looks for a domain controller that can authenticate and synchronize time with the client. When a domain controller is found, the client sends a request for time and waits for a reply from the domain controller. This communication is

an exchange of Simple Network Time Protocol (SNTP) packets intended to calculate the time offset and roundtrip delay between the two computers.

How the Windows Time service communicates with sites on the Internet

The Windows Time service automatically synchronizes the local computer's time with other computers on the network. The time source for this synchronization varies, depending on whether the computer is joined to a domain in the Active Directory directory service or to a workgroup.

When a computer running Windows 2000 is a member of a domain

In this scenario, the Windows Time service configures itself automatically, using the Windows Time service that is available on the domain controllers.

The Windows Time service on a domain controller can be configured as either a reliable or an unreliable time source. The Windows Time service running on a client will attempt to synchronize its time source with servers that are indicated as reliable. The Windows Time service can configure a domain controller within its domain as a reliable time source, and it synchronizes itself periodically with this source. These settings can be modified or overwritten, depending on specific needs.

When a computer running Windows 2000 is not a member of a domain

The Windows Time service must be manually started for computers running Windows 2000 that are not members of a domain. Computers running Windows 2000 use the Simple Network Time Protocol (SNTP).

The following list describes various aspects of the Windows Time service data that is sent to and from the Internet and how the exchange of information takes place:

- **Specific information sent or received**: The service sends information in the form of a Simple Network Time Protocol (SNTP) packet. For more information about Windows Time service and SNTP packets, see the references listed in "Related documentation and links" later in this section.
- **Default settings**: Computers that are members of an Active Directory domain synchronize time with domain controllers by default. Domain controllers synchronize time with their parent domain controller. By default, the root parent domain controller will not synchronize to a time source. The root parent domain controller can be set to either synchronize to a known and trusted Internet-based time source, or a hardware time device that provides an NTP (Network Time Protocol) or SNTP interface. Its time accuracy can also be maintained manually.
- **Triggers and user notification**: The Windows Time service is started when the computer starts. Additionally, the service will continue to synchronize time with the designated network time source and adjust the computer time of the local computer when necessary. Notification is not sent to the user.
- **Logging**: Information related to the service is stored in the Windows System event log. The time and network address of the time synchronization source is contained in the Windows

event log entries. Additionally, warning or error condition information related to the service is stored in the Windows System event log.

- **Information storage**: The service does not store information, as all information that results from the time synchronization process is lost when the time synchronization service request is completed.
- **Encryption**: Encryption is not used in the network time synchronization for domain peers.
- **Protocol**: The service on Windows 2000 implements SNTP to communicate with other computers on the network.
- **Port**: NTP and SNTP defaults to using User Datagram Protocol (UDP) port 123. If this port is not open to the Internet, you cannot synchronize your server to Internet SNTP servers.
- **Ability to disable**: Disabling the service has no direct effect on applications or other services. Applications and services that depend on time synchronization, such as Kerberos V5 authentication protocol, may fail, or they may yield undesirable results if there is a significant time discrepancy among computers. Because most computers' hardware-based clocks are imprecise, the difference between computer clocks on the network usually increases over time.

Controlling the Windows Time service to limit the flow of information to and from the Internet

The synchronization type and NTP time server information can be managed and controlled through the Windows 2000 registry. The procedures for configuring the Windows Time service are given later in this section of the white paper. When the synchronization type is set to Nt5DS, the Windows Time service synchronizes its time resource with the network domain controller. Alternatively, setting the type attribute to NTP configures the Windows Time service to synchronize with a specified NTP time server. The NTP server is specified by either its Domain Name System (DNS) name or its IP address when you select NTP as the synchronization type.

For more general information about the Windows Time service, see "The Windows Time Service" on the Microsoft Web site at:

www.microsoft.com/windows2000/techinfo/howitworks/security/wintimeserv.asp

Clients on a managed network can be configured to synchronize computer clock settings to an NTP server on the network to minimize traffic out to the Internet and to ensure that the clients synchronize to a single reliable time source. If you choose to do so, you can disable time synchronization for both non-domain and domain computers running Windows 2000 by using the Windows 2000 registry. The procedures for configuring the Windows Time service are given later in this section of the white paper.

How the Windows Time service can affect users and applications

Windows components and services depend on time synchronization. For example, the Kerberos V5 authentication protocol (supported on Windows 2000) on a Windows 2000 domain has a default time synchronization threshold of five minutes. Computers that are more than five minutes out of synchronization on the domain will fail to authenticate using the Kerberos protocol. This time value is also configurable, allowing for shorter or longer thresholds. Failure to authenticate using the Kerberos protocol can prevent logons, access to Web sites, file shares, printers, and other resources or services within a domain.

When the local clock offset has been determined, the following adjustments are made to the time:

- If the local clock time of the client is behind the current time received from the server, the Windows Time service will change the local clock time immediately.
- If the local clock time of the client is more than three minutes ahead of the time on the server, the service will change the local clock time immediately.
- If the local clock time of the client is less than three minutes ahead of the time on the server, the service will quarter or halve the clock frequency for long enough to synchronize the clocks.
- If the client is less than 15 seconds ahead, it will halve the frequency; otherwise, it will quarter the frequency. The amount of time the clock spends running at an unusual frequency depends on the size of the offset that is being corrected.

Configuration settings for the Windows Time service

You can set the global configuration settings for the Windows Time service by modifying the entries in the Windows 2000 registry. For more information about the Windows Time service and the registry, see "Registry Entries for the W32Time Service" on the Microsoft Web site at:

support.microsoft.com/default.aspx?scid=kb;en-us;Q223184

Notes
To modify entries in the Windows 2000 registry, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Administrators group might be able to modify the registry. As a security best practice, consider using Run as when modifying the registry.

To open Registry Editor, click **Start**, click **Run**, and then type **regedit**.

The computer registry values for Windows 2000 listed in this subsection are located in the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

The following table describes the values that can be set:

Registry settings for Windows Time service on computers running Windows 2000

Entry name	Data type	Description and values
ReliableTimeSource	REG_DWORD optional	Used to indicate that this computer has reliable time. 0 = Do not mark computer as reliable. [default = 0] 1 = Mark computer as reliable. This is only useful on a domain controller.
Period	REG_DWORD or REG_SZ	Used to control how often the time service synchronizes. If a value is given, it must be one of the following special values: 65531, "DailySpecialSkew" = once every 45 minutes until successful one time, then once every day 65532, "SpecialSkew" = once every 45 minutes until

		successful three times, then once every eight hours (three times per day) [default] 65533, "Weekly" = once every week (seven days) 65534, "Tridaily" = once every three days 65535, "BiDaily" = once every two days 0 = once per day *freq* = *freq* times per day. If you choose to add a value other than any of those specified above, you must use this option.
AvoidTimeSyncOnWan	REG_DWORD optional	Used to prevent the computer from synchronizing from a computer that is in another site and thus connected by a costly temporary connection. 0 = The site of the time source is ignored. [default = 0] 1 = The computer will not synchronize with a time source that is in a different site.
LocalNTP	REG_DWORD	Used to start the SNTP server. 0 = Do not start server unless this computer is a domain controller. [default = 0] 1 = Always start server.
Type	REG_SZ	Used to control how a computer synchronizes. Nt5DS = Synchronize to domain hierarchy or manually configured source. [default = Nt5DS] NTP = Synchronize to manually configured source. NoSync = Do not synchronize.
NtpServer	REG_SZ optional	Used to manually configure the time source. This can be set to the DNS name or IP address of the server from which to synchronize. Only one DNS name or IP address can be specified. This can be modified from the command line. [default = blank]
GetDcBackoffMinutes	REG_DWORD optional	The initial number of minutes to wait before looking for a domain controller (time source) if the last attempt to find a domain controller failed. [default = 15]
GetDcBackoffMaxTimes	REG_DWORD optional	The maximum number of times to double the backoff interval when successive attempts to find a domain controller fail. An event is logged every time a wait of the maximum length occurs. If the value of this entry is 0, then the wait between successive attempts is always the minimum and no event is logged. [default = 7] The time service tries to find a domain controller according to its usual synchronization schedule, but if the backoff interval has not expired, then that attempt will be skipped. For example, if given the default values, the backoff interval will follow this pattern: 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 16 hours, etc. The time service will, however, only attempt to synchronize on 45-minute intervals, so the attempts to find a domain controller will actually occur after 45 minutes, 1 hour 30 minutes, 2 hours 15 minutes, 4 hours 30 minutes, 8 hours 15 minutes, 16 hours 30 minutes, etc.

Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

Procedures for configuring the Windows Time service

The following procedures explain how to:

- Start and stop the Windows Time service.
- Synchronize the Windows Time service with a specific time source.

Starting and Stopping the Windows Time service

By default, the Windows Time service starts automatically at system startup. You can, however, start or stop the service manually by accessing services in Administrative Tools or by using the **net** command.

To manually start the Windows Time service using the graphical interface

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. Select **Windows Time** from the list of services.
4. On the **Action** menu, click **Start** to begin the service.

To manually stop the Windows Time service using the graphical interface

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. Select **Windows Time** from the list of services.
4. On the **Action** menu, click **Stop** to discontinue the service.

To manually start the Windows Time service using the net command

1. Open **Command Prompt**.
2. At the command prompt, type **net start w32time**, and then press ENTER.

To manually stop the Windows Time service using the net command

1. Open **Command Prompt**.
2. At the command prompt, type **net stop w32time**, and then press ENTER.

Synchronizing Windows Time service with a specific time source

The following procedures explain how to synchronize the Windows Time service with a specific time source.

To synchronize an internal time server with an external time source

1. Open **Command Prompt**.
2. Type the following, where *PeerList* is a comma-separated list of Domain Name System (DNS) names or IP addresses of the desired time sources:
   At the command prompt, type **w32tm /config /syncfromflags:manual /manualpeerlist:***PeerList*, and then press ENTER.
3. At the command prompt, type **w32tm /config /update**, and then press ENTER.

Notes
The most common use of this procedure is to synchronize the internal network's authoritative time source with precise external time source. This procedure can be run on any computer running Windows 2000.

If the computer cannot reach the servers, the procedure fails and an entry is written to the Windows System event log.

To synchronize the client time with a time server

1. Open **Command Prompt**.
2. At the command prompt, type **w32tm /resync**, and then press ENTER.

Notes
This procedure only works on computers that are joined to a domain.

The W32tm command-line tool is used for diagnosing problems that can occur with the Windows Time service. If you are going to use this tool on a domain controller, it is necessary to stop the service. Running the tool and the Windows Time service at the same time on a domain controller generates an error because both are attempting to use the same UDP port. When you finish using the W32tm command-line tool, the service must be restarted.

Monitoring and troubleshooting the Windows Time service

In many cases problems with the Windows Time service can be attributed to network configuration. If the network is not configured correctly computers might not be able to communicate to send time samples back and forth. Viewing the contents of NTP packets can help you to identify exactly where a packet is blocked on a network. An error associated with the Windows Time service might occur when a computer is unable to synchronize with an authoritative source. You can use the W32tm command-line tool to assist you in troubleshooting this and other types of errors associated with the Windows Time service.

The W32tm command-line tool is the preferred tool for configuring, monitoring, and troubleshooting the Windows Time service. All tasks that can be performed by using the **net** command can be accomplished by using this tool. For more information about the tool, see the instructions in "Procedure for viewing information about the W32tm command-line tool" later in this section.

Procedure to follow when a computer is unable to synchronize

A computer running the Windows Time service refuses to synchronize if the computer's time is more than 15 hours off. Such occurrences are rare, and are often caused by configuration setting errors. For example, if a user sets the date on the computer incorrectly, the time does not synchronize. Under these circumstances, most often the time is off by a day or more. Be sure to check the computer's calendar and ensure that the correct date has been set.

To resynchronize the client time with a time server

1. Click **Start**, point to **All Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, type **w32tm /resync /rediscover**, and then press ENTER.

Notes
When you run the preceding command, it redetects the network configuration and rediscovers network resources, causing resynchronization. This procedure only works on computers that are joined to a domain. You can then view the event log for more information about why the time service does not synchronize. For more information about the W32tm command-line tool, see the next subsection, "Procedure for viewing information about the W32tm command-line tool."

The tool is used for diagnosing problems that can occur with the Windows Time service. If you are going to use the tool on a domain controller, it is necessary to stop the service. Running the tool and the Windows Time service at the same time on a domain controller generates an error because both are attempting to use the same UDP port. When you finish using the W32tm command-line tool, the service must be restarted.

Procedure for viewing information about the W32tm command-line tool

Accessing the Windows 2000 Help documentation

Windows 2000 has Help documentation describing how to view Help information for command-line tools. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any server running Windows 2000. The following procedure gives the details.

To access the Help documentation for a server running Windows 2000

1. Open Help for Windows 2000 by doing one of the following:
   - On any computer running Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server, click **Start**, and then click **Help**. Click the **Contents tab**. If the Contents tab is not showing, click **Show**, and then click the **Contents tab**.
   - View Help on the Web at:

     www.microsoft.com/windows2000/techinfo/proddoc/
2. Locate the specific topic as follows:
   - To display the Help information for the W32tm command-line tool, navigate to Troubleshooting and Additional Resources\Additional Resources\Windows 2000 commands\Help.

Related documentation and links

- For more information about the Windows Time service, see the following pages on the Microsoft Web site at:

  www.microsoft.com/windows2000/techinfo/howitworks/security/wintimeserv.asp

  www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/operate/wintime.asp

- For more information about the Windows Time service and the registry, see "Registry Entries for the W32Time Service" on the Microsoft Web site at:

  support.microsoft.com/default.aspx?scid=kb;en-us;Q223184

Using online resources. The Microsoft Web site contains support information, including the latest downloads and Knowledge Base articles written by support professionals at Microsoft:

- You can search frequently asked questions (FAQs) by product, browse the product support newsgroups, and contact Microsoft Support at the following Web site. You can also search the Microsoft Knowledge Base of technical support information and self-help tools for Microsoft products at this site:

  support.microsoft.com/

- You can search for troubleshooting information, service packs, patches, and downloads for your system on the Technet Web site at

  www.microsoft.com/technet/

Windows Update and Automatic Updates

This section provides information about:

- The benefits of Windows Update and Automatic Updates
- How Windows Update and Automatic Updates communicate with sites on the Internet
- How to control Windows Update and Automatic Updates to limit the flow of information to and from the Internet

Benefits and purposes of Windows Update and Automatic Updates

Windows Update

Windows Update is an online catalog customized for computers running Microsoft Windows 2000 Service Pack 3 (SP3) that consists of items such as drivers, critical updates, Help files, and Internet products. Windows Update scans the user's computer and provides a tailored selection of updates that apply only to the software and hardware on that specific computer. Windows Update then enables users to choose updates for their computer's operating system and hardware. New content is added to the Windows Update Web site regularly, so users can always get the most recent and secure updates and solutions.

Windows Update contains two key components:

- **Content update**: Content updates occur when the user accesses the Windows Update Web site and selects component updates to download and install. The user is fully aware of downloads to the computer. The Windows Update Web site is located at:

  windowsupdate.microsoft.com/

- **Web service control update**: The Windows Update Web service includes an ActiveX Web control program that downloads and installs the content updates. The Windows Update team receives feedback from their customers on how to improve their Web service and the Windows Update service control is changed to reflect that feedback. In order to access the new content and services customers need, the Web controls are updated periodically. This service automatically downloads a new version of the Web control program when the user visits the Windows Update site or when any of the other Windows features calls on the Windows Update control. Just like downloading an ActiveX control, the user may receive a security dialog box that a Web control is attempting to be installed. Users may not receive the dialog box if they have selected to always trust Microsoft as a content provider (using their security settings in Microsoft Internet Explorer). If users do not click Yes on the security dialog box, the control will not be updated.

Automatic Updates

This option for updating a computer allows for updates without interrupting the user's Web experience. Automatic Updates is not enabled by default; users are prompted to enable this option following setup. When Automatic Updates is enabled, users do not need to visit special

Web pages or remember to periodically check for new updates. An icon appears in the notification area each time new updates are available. Updates can be downloaded in the background with minimal impact on the user's network connections. Once the update is downloaded, Windows 2000 SP3 prompts the user to install it. Users can set Automatic Updates options in one of three ways to control how and when they want Windows 2000 SP3 to update their computers. They can:

- Choose to have Windows 2000 SP3 send a notification before downloading and installing any updates.
- Choose to have Windows 2000 SP3 download and install updates automatically on a schedule that they specify.
- Choose to have Windows 2000 SP3 send a notification whenever it finds updates available for their computers. Windows 2000 SP3 will then download the updates in the background, enabling users to continue working uninterrupted. After the download is complete, an icon in the notification area will prompt users that the updates are ready to be installed.

Users can choose not to install a specific update that has been downloaded; in that case, Windows 2000 SP3 will delete those files from the computer. Users can download those deleted files again by opening Control Panel, clicking **Automatic Updates**, and then clicking **Declined Updates**. If any of the updates users previously declined can still be applied to their computers, they will appear the next time Windows 2000 SP3 notifies those users of available updates.

Alternatives to Windows Update and Automatic Updates

For managed environments, there are several alternatives to Windows Update:

- Windows Update Catalog Web site.
- Microsoft Software Update Services (SUS).
- Distribution software, such as Microsoft Systems Management Server, that can be used to distribute software updates. For more information, see the documentation for your distribution software, and see Appendix A, "Resources for Learning About Automated Installation and Deployment," especially the "Related documentation and links" subsection in that appendix.

Windows Update Catalog Web site

You can deploy updates to Windows in a managed environment without requiring users to connect to the Windows Update Web site by using the Windows Update Catalog site, located at:

corporate.windowsupdate.microsoft.com

The Windows Update Catalog site provides a comprehensive catalog of updates that can be distributed over a managed network. It provides a single location for Windows Update content and drivers that display the Designed for Windows logo. Administrators can search the site using keywords or predefined search criteria to select the relevant downloads and then to download the updates to a location on their internal network.

Microsoft Software Update Services (SUS)

Microsoft Software Update Services (SUS) is a version of Windows Update designed for installation inside an organization's firewall. This feature is very useful for organizations that:

- Do not want their systems or users connecting to an external Web site
- Want to first test these updates before deploying them throughout their organization

Microsoft Software Update Services enables administrators to quickly and reliably deploy critical updates to their Windows 2000-based servers as well as desktop computers running Windows 2000 Professional.

For more information about software update services, see the Microsoft Web site at:

www.microsoft.com/windows2000/windowsupdate/sus/default.asp

Overview: Using Windows Update and Automatic Updates in a managed environment

Users have control over whether to enable Automatic Updates following setup, and they also have direct control over accepting downloaded files from Windows Update. In a managed environment, however, it is unlikely that users will be allowed unlimited access to install updated drivers and other updated files; this function would normally be controlled in some fashion by the IT department. You can use Group Policy to block users from accessing Windows Update in the user interface or to specify an internal server for Windows Update to use when searching for updates. You can also disable Automatic Updates using Control Panel or Group Policy. Details on the methods and procedures for controlling these features are described in the following subsections.

How Windows Update and Automatic Updates communicate with sites on the Internet

This subsection summarizes the communication process:

- **Specific information sent or received**: Drivers and replacement files (critical updates, Help files, and Internet products) may be downloaded to the user's computer. The computer is uniquely identified and is logged in the download and installation success report, but the user is not uniquely identified.
- **Data storage and access**: Windows Update tracks the total number of unique computers that visit the Windows Update Web site. The success or failure of downloading and installing updates is also recorded but no personally identifiable information is recorded as part of this. This information is stored on Microsoft servers with limited access that are located in controlled facilities. No other information collected during a Windows Update session is retained past the end of the session.

  For more information, see "Privacy policy," later in this list.

  Note If you want to block the use of the Windows Update Web site, you can apply Group Policy settings to specify an internal server for updates and for storing upload statistics. For more information, see "Procedures for disabling Windows Update and Automatic Updates."

- **Default and recommended settings**: By default, Windows 2000 SP3 allows access to the Windows Update Web site. Recommended settings are described in the next subsection, "Controlling Windows Update and Automatic Updates to limit the flow of information to and from the Internet."

- **Triggers**: The user controls whether to run Windows Update. If Automatic Updates is enabled following setup, it is triggered about once per day when there is an Internet connection.
- **User notification**:
  - **Windows Update**: Users are notified when Windows Update downloads files to their computer, and they have control over whether to install those downloads.
  - **Automatic Updates**: Administrators can specify one of two notification settings for Automatic Updates:
    - Notify users before downloading and installing any updates.
    - Download the updates automatically and notify users when they are ready to be installed.

  Note Administrators can also specify that updates be automatically downloaded and installed following a set schedule without user notification. For more information about these settings, click the **Learn more about automatic updating** link on the Automatic Updates dialog box.

- **Logging**: Automatic Updates logs events to the event log.
- **Encryption**: The data is transferred using HTTPS. The data packages downloaded to the user's system by Microsoft are digitally signed.
- **Privacy policy**: To view the privacy policy for Windows Update, see the Windows Update Web site, and click **Read our privacy statement**. The Windows Update Web site is located at:

  windowsupdate.microsoft.com/

  Automatic Updates is covered by the same policy that covers Windows Update.
- **Transmission protocols and ports**: The transmission protocols and ports used are HTTP 80 and HTTPS 443.
- **Ability to disable**: You can use Group Policy to remove user access to Windows Update in the user interface. You can use Group Policy to specify an internal server to use for Windows Update and block it from searching the Windows Update Web site. You can disable Automatic Updates using Control Panel tools or Group Policy. Procedures for these methods are given at the end of this section.

Controlling Windows Update and Automatic Updates to limit the flow of information to and from the Internet

The recommended methods for controlling Windows Update or Automatic Updates or both are as follows:

- You can use Group Policy settings to control Windows Update and Automatic Updates by removing end user access to Windows Update.
- You can block Windows Update from searching the Windows Update Web site by using Group Policy settings to specify an internal server for updates.
- You can use Control Panel or Group Policy settings to selectively disable Automatic Updates.

- You can control both Windows Update and Automatic Updates by blocking HTTP port 80 or HTTPS port 443 or both at the firewall.

See the following table for more information about the configuration options.

Configuration settings for Windows Update and Automatic Updates

Automatic Updates: Configuration tool	**Setting**	**Result**
Control Panel (Automatic Updates tool)	On the **Automatic Updates** dialog box, clear **Keep my computer up to date**.	Disables Automatic Updates.
Group Policy	Disable the **Configure Automatic Updates** policy setting in the Wuau.adm Group Policy template. For more information, see "Procedures for disabling Windows Update and Automatic Updates" later in this section.	Disables Automatic Updates.
Windows Update and Automatic Updates: Configuration tool	**Setting**	**Result**
Firewall	Block HTTP port 80 or HTTPS port 443 or both.	Blocks Windows Update and Automatic Updates.
Group Policy	Enable the **Remove access to use all Windows Update features** policy setting in the Wuau.adm Group Policy template. For more information, see "Procedures for disabling Windows Update and Automatic Updates" later in this section.	Blocks the user from accessing Windows Update in the Windows 2000 SP3 user interface. Also blocks Automatic Updates.
Group Policy	Enable the **Specify intranet Microsoft update service location** policy setting in the Wuau.adm Group Policy template. For more information, see "Procedures for disabling Windows Update and Automatic Updates" later in this section.	Blocks Windows Updates from searching for updates on the http://windowsupdate.microsoft.com Web site. Instead, Windows Update searches for updates on a specified internal server.

How controlling Windows Update and Automatic Updates can affect users and applications

When you remove user access to Windows Update, Windows will still search for and download updates to the local computer. Users will not, however, be able to access the Windows Update Web site by clicking **Start** and then **Windows Update**, or from the Tools menu in Microsoft Internet Explorer, or from the Windows Update button in Add/Remove Programs. They will also not be prompted to install downloaded updates. In addition, removing user access to Windows Update also disables Automatic Updates; that is, the user for which this policy setting is enabled will neither be notified about nor will receive critical updates from Windows Update. Removing user access to Windows Update is a user-based, not system-based, policy; other users on the same computer will still receive critical updates unless this policy setting is also enabled for those users individually.

Removing end user access to Windows Update also prevents Device Manager from automatically installing driver updates from the Windows Update Web site. For more information about controlling Device Manager, see the section of this white paper titled "Device Manager."

Blocking Windows Update and Automatic Updates will not block applications from running.

The Windows Update site is located at:

windowsupdate.microsoft.com/

Procedures for disabling Windows Update and Automatic Updates

This subsection provides procedures for following configurations:

- Specifying that Windows Update search an internal server, rather than the Windows Update Web site, for updates.
- Removing user access to Windows Update by using Group Policy, which will also block Automatic Updates.
- Disabling Automatic Updates by using Group Policy.
- Disabling Automatic Updates by using Control Panel tools.

To specify an internal server for Windows Update using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Update**.
3. In the details pane, double-click **Specify intranet Microsoft update service location**, supply the name of the internal server to function as the update server, and supply the name of the server to store upload statistics.
4. Click **Enabled**.

Important The upgrade server and the server you specify to store upload statistics can be the same server.

To remove user access to Windows Update using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."

2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Update**.
3. In the details pane, double-click **Remove access to use all Windows Update features**, and then click **Enabled**.

Important Removing user access to Windows Update also disables Automatic Updates.

To disable Automatic Updates using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for Learning About Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Update**.
3. In the details pane, double-click **Configure Automatic Updates**, and then click **Disabled**.

To disable Automatic Updates using Control Panel tools

1. Click **Start**, and then point to **Settings,** and then click **Control Panel**.
2. Click **Automatic Updates**.
3. On the **Automatic Updates** dialog box, clear the **Keep my computer up to date** check box.

Appendices

Appendix A: Resources for Learning About Automated Installation and Deployment

The following appendix provides:

- An overview of automated installation and deployment
- Information about using integrated installation
- Procedures and resources for obtaining more information about automated installation and deployment

Overview: Automated installation and deployment

In the enterprise environment, it is not cost-effective to install Microsoft Windows 2000 Service Pack 3 (SP3) using the standard interactive setup on each computer. To greatly lower the total cost of ownership (TCO) and to ensure configuration uniformity, you can perform an automated installation of Windows 2000 SP3 on multiple computers. By using an automated installation method, you can ensure that certain components and applications are not available on your organization's computers, or that certain components and applications are preconfigured in such a way that helps prevent unwanted communication over the Internet.

Notes
In addition to the automated installation methods described here, another common method of controlling Internet connections is to use a script to configure Group Policy on each client computer. The script can be sent to each client computer using a tool such as Microsoft Systems Management Server (SMS) and can run remotely using Windows Script Host. Alternatively, Group Policy can be applied to a domain, site, or organizational unit. The policy settings would then automatically be applied to every computer in the domain, site, or organizational unit the first time the computer starts after the operating system is installed. For more information about scripts and Group Policy, see "Related documentation and links" at the end of this section.

You can also use scripts to monitor activity on client computers and to take appropriate action if certain restricted activities occur. For example, if a user were to start an unauthorized application, a script could be used to detect this and to immediately stop that application. Similarly, scripts can be used to monitor the setup of each computer in order to, for example, determine what applications are installed and what folders are being shared. Configuring these scripts is beyond the scope of this document; however, you can refer to "Related documentation and links" at the end of this section for more information.

There are several options for automating the setup process. Any or all of the following tools can help ensure that all of your client computers are configured to appropriately limit communication over the Internet:

- Unattended setup using Setup (Winnt32.exe)

  Unattended setup enables you to simplify the process of setting up the operating system on multiple computers by running Setup unattended. To do this, you can create and use an answer file, which is a customized script that answers setup questions automatically. Then

you can run Setup (Winnt32.exe) from the command line with the appropriate options for invoking unattended setup.

Using Winnt32.exe, you can upgrade your previous version of the operating system using all user settings from the previous installation, or you can perform a fresh installation using the answer file that provides setup with your custom specifications. The latter method is most likely the best option to limit component communication over the Internet, provided you use an appropriate answer file. Details about specific answer file entries are included in the appropriate component sections of this white paper.

- Remote Installation Services (RIS)

  You can use RIS to create installation images of operating systems or of complete computer configurations, including desktop settings and applications. You can then make these installation images available to users at client computers. You can also specify which RIS server will provide installations to a given client computer, or you can allow any RIS server to provide the installation.

- Image-based installation using the System Preparation (Sysprep) tool.

  Image-based installation is also a good choice if you need to install an identical configuration on multiple computers. On a master computer, you install the operating system and any applications that you want installed on all of the target computers. Then you run Sysprep and a disk imaging utility. Sysprep prepares the hard disk on the master computer so that the disk imaging utility can transfer an image of the hard disk to the other computers. This method decreases deployment time dramatically compared to standard or scripted installations. You can customize the images so that only the files required for a specific configuration appear on the image, such as additional Plug and Play drivers that might be needed on various systems. The image can also be copied to a CD and distributed to remote sites that have slow links.

- System management software, such as Microsoft Systems Management Server (SMS)

  This software assists with the many tasks that are involved when you apply automated procedures to multiple servers and client computers throughout your organization. These tasks include:

  - Selecting computers that are equipped for the operating system and that you are ready to support.
  - Distributing the operating system source files to all sites, including remote sites and sites without technical support staff.
  - Monitoring the distribution to all sites.
  - Providing the appropriate user rights to do the upgrade.
  - Automatically initiating the installation of the software package with the possibility of having the user control the timing.
  - Resolving problems related to the distributions or installations.
  - Reporting on the rate and success of deployment.

Using system management software helps to further ensure that all computers within your organization have received the standardized operating system configuration that helps prevent unwanted communication over the Internet.

Integrated installation

During setup, you can apply SP3 directly to the Windows 2000 installation files and complete an integrated installation, rather than applying SP3 after the initial installation of Windows 2000. Integrated installation can be done as part of an automated installation process. One of the advantages of using integrated installation is that with this method, you can remove access to Microsoft Internet Explorer, Outlook Express, or Windows Media Player either during unattended installation for Windows 2000 or while running Sysprep for Windows 2000. (These components cannot be automatically removed during an installation of Windows 2000 independent of SP3.) For more information about the integrated installation methods for SP3, see the Service Pack 3 Installation and Deployment Guide on the following Web site at:

www.microsoft.com/windows2000/downloads/servicepacks/sp3/spdeploy.htm

Procedures for accessing additional information about other automated setup tools

Accessing the Windows 2000 Help documentation

Windows 2000 has Help documentation describing unattended installation, RIS, and image-based installation. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any server running Windows 2000. The following procedure gives the details.

To access the Help documentation for a server running Windows 2000

1. Open Help for a product in the Windows 2000 Server family by doing one of the following:
   - On any computer running Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server, click **Start**, and then click **Help**. Click the **Contents** tab. If the Contents tab is not showing, click **Show**, and then click the **Contents** tab.
   - View Help on the Web at:

     www.microsoft.com/windows2000/techinfo/proddoc/
2. Locate the specific topics as follows:
   - For unattended installation: Navigate to Getting Started with Windows 2000 Server\Installing Windows 2000 Server\Concepts\Planning for unattended setup.
   - For RIS: Navigate to Users and Computers\Remote Installation Services.

Related documentation and links

You can also find additional information about all of the topics described earlier in this appendix in a variety of other locations:

- For more information about answer file parameters and syntax, see "Microsoft Windows 2000 Guide to Unattended Setup" (Unattend.doc) on the Microsoft Windows 2000 operating system CD. The Unattend.doc file is in the \Support\Tools folder on the CD.
- The Windows 2000 Help documentation on the Web includes information about Winnt32.exe at:

www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/wgs_gs_03016.htm

- For more information about the System Preparation (Sysprep) tool, see the MSDN article "Automating Windows 2000 Installations with Sysprep" at:

  msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kmag00/html/Sysprep.asp

- For extensive information about unattended setup and Systems Management Server, see the following topics in the Windows 2000 Resource Kit on the Web:

  - "Automating Server Installation and Upgrade" at:

    www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dgcb_ins_adeb.asp

  - "Using Systems Management Server to Deploy Windows 2000" at:

    www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dggf_sms_zunm.asp

- For general information about Group Policy, see Appendix B, "Resources for Learning About Group Policy."

- For information about deployment, see the planning and deployment page for Windows 2000, as well as the Windows 2000 Deployment Guide. These can be viewed at:

  - www.microsoft.com/windows2000/techinfo/planning/default.asp

  - www.microsoft.com/windows2000/techinfo/reskit/en-us/w2rkbook/DPG.asp?frame=true

- The Windows 2000 Help documentation included on the CD and on the Web includes information about Windows Script Host. You can find the documentation on the Web at:

  www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/sag_WSHtopnode.htm

Appendix B: Resources for Learning About Group Policy

The following appendix provides:

- An overview of Group Policy
- Procedures for obtaining more information about Group Policy

Overview: Group Policy

As described in earlier sections of this white paper, you can use Group Policy to configure many Microsoft Windows 2000 Service Pack 3 (SP3) components in a way that will prevent users from accessing these components, or alternatively, in a way that will control how these components exchange data over the Internet. Group Policy settings define the various aspects of the user's desktop environment that a system administrator can manage; for example, the applications that are available to users and how those applications operate.

Group Policy includes **User Configuration** policy settings, which affect users, and **Computer Configuration** policy settings, which affect computers. Using Group Policy you can, among other tasks:

- Make certain Windows components unavailable to particular users.
- Assign scripts (such as computer startup and shutdown, and logon and logoff).
- Specify security options.
- Manage registry-based policy settings through Administrative Templates. Group Policy creates a set of default files that contain registry settings that are written to the User or Local Machine portion of the registry database. In addition, you can create custom Administrative Templates further extending policy settings. User settings that are specific to a user who logs on to a given workstation or server are written to the registry under HKEY_CURRENT_USER (HKCU). Computer-specific settings are written under HKEY_LOCAL_MACHINE (HKLM).

How and when Group Policy is applied

User policy settings are obtained when a user logs on. Computer policy settings are obtained when a computer boots.

Order of application

Policy settings are applied in this order:

1. The unique local Group Policy object (GPO). (A GPO is a collection of policy settings.)
2. Group Policy objects for sites, in administratively specified order.
3. Group Policy objects for domains, in administratively specified order.
4. Group Policy objects for organizational units, from the largest to the smallest organizational unit (parent to child organizational unit), and in administratively specified order at the level of each organizational unit.

By default, policy settings applied later overwrite previously applied policy settings when there is an inconsistency. If the policy settings are not inconsistent, however, earlier and later policy settings both contribute to the effective policy.

Blocking policy inheritance

Policy settings that would otherwise be inherited from higher site, domain, or organizational units can be blocked at the site, domain, or organizational unit level.

Enforcing policy from above

Policy settings that would otherwise be overwritten by policy settings in child organizational units can be set to **No Override** at the Group Policy object level. Policy settings set to **No Override** cannot be blocked.

Procedures for accessing additional information about Group Policy

Accessing the Group Policy Help documentation for Windows 2000 SP3

Windows 2000 SP3 has extensive Help documentation describing Group Policy concepts and procedures. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any computer running a product in the Windows 2000 Server family with SP3. The following procedure describes details.

To view Group Policy Help documentation for computers running a product in the Windows 2000 Server family with SP3

1. Open Help by doing one of the following:
   - On any computer running a product in the Windows 2000 Server family with SP3, click **Start**, and then click **Help**. Click the **Contents** tab. If the **Contents** tab is not showing, click **Show**, and then click the **Contents** tab.
   - View Help on the Web at:

     www.microsoft.com/windows2000/en/server/help/
2. Expand **Users and Computers**.
3. Expand **Group Policy**.

Related links

- For more information about Group Policy, see "Group Policy Reference" in the Windows 2000 Resource Kit at:

  www.microsoft.com/windows2000/techinfo/reskit/en-us/w2rkbook/gp.asp

- Another source of information about Group Policy is the Deployment Planning Guide in the Windows 2000 Server Resource Kit. The chapters that are most relevant are in Part 6, "Windows 2000 Professional/Client Deployment," and are called "Defining Client Administration and Configuration Standards" and "Applying Change and Configuration Management." You can view the Deployment Planning Guide on the Web at:

  www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dgfa_pt6_fhpz.asp

- For information about how to create your own Administrative Templates for controlling application settings, see the white paper titled "Implementing Registry-Based Group Policy" at:

  www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp

Appendix C: Certificate Components

Certificates can play an important role in a network where security is a high priority. This section provides information about:

- The benefits of certificate components in Microsoft Windows 2000 Service Pack 3 (SP3)
- Resources for learning about certificates and public key infrastructure

Benefits and purposes of the certificate components in Windows 2000 SP3

Certificates, and the public key infrastructure of which they are a part, support authentication and encrypted exchange of information on open networks, such as the Internet, extranets, and intranets. A certificate securely binds a public key to the entity that holds the corresponding private key. With certificates, host computers on the Internet no longer have to maintain a set of passwords for individual subjects who need to be authenticated as a prerequisite to access. Instead, the host merely establishes trust in a certification authority. The host can establish this trust through a certificate hierarchy that is ultimately based on a root certificate, that is, a certificate from an authority that is trusted without assurances from any other certification authority.

Examples of times that a certificate is used are when a user:

- Uses a browser to engage in a Secure Sockets Layer (SSL) session
- Accepts a certificate as part of installing software
- Accepts a certificate when receiving an encrypted or digitally signed e-mail message

When learning about public key infrastructure, it is important to learn not only about how certificates are issued, but how certificates are revoked, and how information about those revocations is made available to clients. This is because certificate revocation information is crucial for a user's application that is seeking to verify that a particular certificate is currently (not just formerly) considered trustworthy. Certificate revocation information is often stored in the form of a certificate revocation list, although this is not the only form it can take. Applications that have been presented with a certificate might contact a site on an intranet or the Internet for information not only about certification authorities, but also for certificate revocation information.

In an organization where clients and servers run products in the Windows 2000 family, you have a variety of options in the way certificates and certification revocation lists (or other forms of certificate revocation information) are handled. For more information about these options, see the next subsection, "Resources for learning about certificates and public key infrastructure."

Key aspects of security that certificates support include:

- Authentication, which provides some verification of the identity of someone or something.
- Privacy, which helps ensure that information is available only to the intended audience.
- Encryption, which translates data into code that is extremely difficult to decipher, to help prevent unauthorized readers from accessing the data.

- Digital signatures, which help provide nonrepudiation (that is, making it difficult for the sender to deny that the communication occurred) and message integrity (demonstrating that the message has not been altered since it was signed).

Resources for learning about certificates and public key infrastructure

In an organization where clients and servers run products in the Windows 2000 family, you have a variety of options in the way certificates are handled. For example, you can establish a trusted root authority, also known as a root certification authority, that is inside your organization by using procedures in the documentation sources that follow. The first step in establishing a trusted root authority is to install the Certificate Services component on a server running Windows 2000 SP3. Another step that might be appropriate is to configure the publication of certificate revocation information to the Active Directory directory service. When implementing public key infrastructure, we recommend that you also learn about Group Policy as it applies to certificates.

When you configure a certification authority inside your organization, the certificates it issues can specify a location of your choosing for retrieval of additional evidence for validation. That location can be a Web server or a directory within your organization. Because it is beyond the scope of this white paper to provide full details about certificates and certification authorities, this section provides a list of conceptual information and a list of resources to help you learn about certificates.

Some of the concepts to study when learning about certificates include:

- Certificates and the X.509 V3 standard (the most widely used standard for defining digital certificates)
- Standard protocols that relate to certificates, for example, Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Secure Multipurpose Internet Mail Extensions (S/MIME)
- Encryption keys and how they are generated
- Certification authorities, including the concept of a certification authority hierarchy and the concept of an offline root certification authority
- Certificate revocation
- Ways that Active Directory and Group Policy can work with certificates

The following list of resources can help you as you plan or modify your implementation of certificates and public key infrastructure:

- "Troubleshooting Certificate Status and Revocation," a white paper on the Microsoft Technet Web site at:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp

- Help for Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server.

  You can view the Windows 2000 Help on the Web at:

  www.microsoft.com/windows2000/techinfo/proddoc/

- The Windows 2000 Server Resource Kit, *Deployment Planning Guide* (especially Part 3, "Active Directory Infrastructure," which includes a chapter on public key infrastructure).

  You can view the Windows 2000 Resource Kits on the Windows Deployment and Resource Kits Web site at:

  www.microsoft.com/reskit/

- Links to information about public key infrastructure on the Technet Web site at:

  www.microsoft.com/technet/security/prodtech/pubkey/default.asp

Appendix D: Connection Manager

This section provides information about:

- The benefits of Connection Manager 1.2
- How Connection Manager communicates with sites on the Internet
- Controlling Connection Manager to limit the flow of information to and from the Internet

Benefits and purposes of Connection Manager 1.2

Connection Manager 1.2 is a client dialer and connection software program found in Microsoft Windows 2000 Service Pack 3 (SP3). It provides support for local and remote connections to your service using a network of access points, such as those available worldwide through Internet service providers (ISPs). You can customize Connection Manager by using the Connection Manager Administration Kit (CMAK) wizard, so that the set of files you distribute to your users (called a service profile) can be easily installed and run.

Connection Manager 1.2 supports a variety of features that both simplify and enhance the implementation of connection support for you and your users, most of which can be incorporated using the CMAK wizard.

In addition to the support for basic dial-up connections, you can also use the CMAK wizard to incorporate support for virtual private network (VPN) connections using tunneling protocols to tunnel through a public network (such as when dialing into an ISP to access an organization's server). Connection Manager can create a VPN connection through a preexisting dial-up session, local area network (LAN), or digital subscriber line (DSL).

For more information about Connection Manager, see the instructions in "Accessing the Windows 2000 Help documentation for Connection Manager," later in this appendix.

How Connection Manager communicates with sites on the Internet

The phone book server sends one of the following elements to the Connection Manager client while there is a connection:

- Phone book update file: The server sends a phone book update file when the phone book version of the connecting client is earlier than the version of the phone book server.
- Replacement phone book: This is sent when there is a difference of more than five versions between the client and the server phone book file versions.
- Standard HTTP error message

The following list describes various aspects of the Connection Manager information that is sent to and from the Internet and how the exchange of information takes place:

- **Specific information sent or received**: The information sent by Connection Manager in the phone book server query string contains the following information elements:

  - **osarch**: Specifies the type of processor that the requesting computer is using.
  - **ostype**: Specifies the version of the Windows operating system of the computer making the request.
  - **cmver**: Specifies the version of Connection Manager of the computer making the request.
  - **lcid**: Specifies the locale identifier (LCID) describing the system default locale information of the computer making the request.
  - **pbver**: Specifies the current version of the phone book being used by the computer making the request.
  - **pb**: Specifies the name of the phone book being used by the computer making the request.
- **Default settings**: The Connection Manager client software is installed by default on computers running Windows 2000. The Connection Manager client cannot be used until a Connection Manager service profile is provided to the user.
- **Triggers**: Connection Manager is triggered when users start it to connect to the Internet or their organization's network.
- **Logging**: Information is logged in the Connection Manager log file but not in the Windows 2000 event log. The logging feature for Connection Manager is used for troubleshooting and can be disabled by the user.
- **Encryption**: The information contained in the query string is sent as plaintext and is not encrypted.
- **Access**: The information that is sent is used by the phone book server to process the request being made, although the information is not stored.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You can disable Connection Manager by not providing the user with a Connection Manager service profile. The Connection Manager phone book download and synchronization feature can be disabled by using the CMAK wizard to create a Connection Manager service profile.

For more information about the Connection Manager Administration Kit (CMAK), see "Before you start: Understanding Connection Manager and the Administration Kit" on the Microsoft Web site at:

www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/cmak_ops_03.htm

You can also view the same information in Help, as described in "Accessing the Windows 2000 Help documentation for Connection Manager," later in this appendix.

> **Note** The Connection Manager Administration Kit (CMAK) and the phone book server are optional components that are not installed by default.

Controlling Connection Manager to limit the flow of information to and from the Internet

The Connection Manager client software is installed by default on computers running Windows 2000 (SP3). You can limit the use of Connection Manager by creating and distributing a service profile only to users who need to use the Connection Manager client to initiate local or remote network access point connections. You can use the Connection Manager Administration Kit (CMAK) wizard to create a customized service profile to configure Connection Manager not to update the client phone book information.

The CMAK wizard is designed for network administrators, information officers, and other team members who are responsible for the design, development, testing, distribution, and support of connection software for customers who connect to your Internet or network service.

For more information about the Connection Manager Administration Kit (CMAK), see "Accessing the Windows 2000 Help documentation for Connection Manager," later in this section.

Procedures for installing Connection Manager Administration Kit and for viewing information in Windows 2000 Help

This subsection lists procedures for the following tasks:

- Installing Connection Manager Administration Kit on your server
- Accessing the Windows 2000 Help documentation for Connection Manager

Installing Connection Manager Administration Kit on your server

The Connection Manager Administration Kit (CMAK) and Phone Book Service components are not installed by default on products in the Windows 2000 Server family. Use the following procedure to add the Connection Manager Administration Kit and Phone Book Service to your server running Windows 2000.

To add the Connection Manager Administration Kit and Phone Book Service after server installation.

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Scroll down and double-click **Management and Monitoring Tools**.
5. Make sure the check box for the Connection Manager Components is checked.
6. Follow the instructions to complete the Windows Components Wizard.

Notes

The Connection Manager client software is installed by default on computers running Windows 2000. You can limit the use of Connection Manager by creating and distributing

a service profile only to users who need to use the Connection Manager client to initiate local or remote network of access point connections.

For more information about the Connection Manager Administration Kit (CMAK), see the next procedure, "Accessing the Windows 2000 Help documentation for Connection Manager."

Accessing the Windows 2000 Help documentation for Connection Manager

Windows 2000 has Help documentation describing the Connection Manager Administration Kit. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any server running Windows 2000. The following procedure gives the details.

To access the Help documentation for a server running Windows 2000

1. Open Help for a product in the Windows 2000 Server family by doing one of the following:
   - On any computer running Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server, click **Start**, and then click **Help**. Click the **Contents tab**. If the Contents tab is not showing, click **Show**, and then click the **Contents tab**.
   - View Help on the Web at:

     www.microsoft.com/windows2000/techinfo/proddoc/
2. To view information about Connection Manager Administration Kit, navigate to Connections\Connection Manager Administration Kit.

Related documentation and links

- For more information about the Connection Manager Administration Kit (CMAK), see the following references:
  - "The Connection Manager Administration Kit and the customization process" on the Microsoft Web site at:

    www.microsoft.com/windows2000/en/server/help/default.asp?url=/WINDOWS2000/en/server/help/cmak_ops_12.htm
  - "Before you start: Understanding Connection Manager and the Administration Kit" on the Microsoft Web site at:

    www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/cmak_ops_03.htm
- For more information about Connection Manager, see the following references:
  - "HOW TO: Create a Custom Connection Manager Service Profile in Windows 2000" on the Microsoft Web site at:

    support.microsoft.com/default.aspx?scid=KB;en-us;317593
  - The instructions in "Accessing the Windows 2000 Help documentation for Connection Manager" earlier in this appendix.

Appendix E: Internet Connection Sharing

The Internet Connection Sharing feature of Microsoft Windows 2000 Service Pack 3 (SP3) (excluding Windows 2000 Datacenter Server) is designed for home and small office networks. Information about this feature is presented here so you as an IT administrator can be aware of these potential capabilities within your organization's network.

This appendix includes the following information:

- An overview of Internet Connection Sharing
- How Internet Connection Sharing can be used in a large organization's network
- How to control or prevent the use of Internet Connection Sharing

Overview: Internet Connection Sharing

With Internet Connection Sharing (ICS), an administrator can connect computers on a home or small office network to the Internet using just one connection. For example, you might have one computer that connects to the Internet using a dial-up connection. When ICS is enabled on this computer, called the ICS host, other computers on the network can connect to the Internet through this connection.

Internet Connection Sharing is intended for use in a network where the ICS host computer directs network communication between computers and the Internet. It is assumed that in a home or small office network, the ICS host computer has the only Internet connection.

> **Note** You should not use Internet Connection Sharing in an existing network with Windows 2000 Server-based domain controllers, Domain Name System (DNS) servers, gateways, Dynamic Host Configuration Protocol (DHCP) servers, or systems configured for static IP addresses.

Using Internet Connection Sharing in a managed environment

While Internet Connection Sharing (ICS) is designed for home and small office use, administrators can access this capability in a managed environment. ICS lets administrators configure a computer as an Internet gateway for a small network, and it provides network services, such as name resolution and addressing through DHCP to the local private network.

ICS is disabled by default, but an administrator can enable it by configuring a network connection in Network and Dial-up Connections. To do this you select the **Properties** page for a dial-up, a virtual private network (VPN), or an incoming network connection and then select the **Sharing** tab. On the Sharing tab you select **Enable Internet connection sharing for this connection**. In a managed environment we recommend that you disable this capability using Group Policy.

Controlling the use of Internet Connection Sharing

You can block administrators and users with administrative credentials from accessing this feature by configuring Group Policy. By navigating to Computer or User Configuration\Administrative Templates\Network\Network and Dial-up Connections, you can configure the policy setting **Prohibit configuration of connection sharing**. This policy setting is described as follows:

- You use this policy setting to control whether administrators can enable, disable, and configure the connection sharing feature of a network connection.
- If you enable this policy setting, the system removes the Sharing tab from the Properties dialog box for a connection.
- The policy setting appears in the Computer Configuration and User Configuration folders. If this policy setting is configured in both folders, the one in Computer Configuration takes precedence over the one in User Configuration.

Appendix F: Add Network Place Wizard

In Microsoft Windows 2000 Service Pack 3 (SP3) users can use the Add Network Place Wizard to create shortcuts to shared folders and resources on the network, on Web servers, or on File Transfer Protocol (FTP) servers. The content in this appendix includes the following:

- An overview of the Add Network Place Wizard
- How to control the use of the Add Network Place Wizard

Overview: Add Network Place Wizard

The Add Network Place Wizard is enabled by default for all users. Users access the wizard through My Network Places\Add Network Place or in Windows Explorer through Tools\Map Network Drive.

Users can use the wizard to create a shortcut to a Web site, an FTP site, or other local network connection. To add a shortcut in My Network Places to a folder on a Web server, the Web server must support network places. Support for network places requires the Web Extender Client (WEC) protocol and FrontPage® Server Extensions, or the Web Distributed Authoring and Versioning (WebDAV) protocol and Internet Information Services (IIS). The user must also have read and write access to the Web server.

In a highly managed network environment administrators might want to prevent users from storing or accessing folders on a Web server. You can remove access to the Add Network Place Wizard using Group Policy.

For more information about the WEC and WebDAV protocols, see "Web folders overview" in Windows 2000 Help.

Controlling the use of the Add Network Place Wizard

In Windows 2000, in order to block users from accessing the Add Network Place Wizard you use Group Policy to block all ways but one to connect to another computer (users can still connect to another computer through the Run dialog box).

Configure the following Group Policy setting in User Configuration\Administrative Templates\Windows Components\Windows Explorer: **Remove "Map Network Drive" and "Disconnect Network Drive**.**"** This policy setting does the following:

- It prevents users from using Windows Explorer or My Network Places to connect to other computers or to close existing connections.
- If you enable this policy setting, the system removes the Map Network Drive and Disconnect Network Drive commands from the toolbar and Tools menus in Windows Explorer and My Network Places. The system also removes these commands from menus that appear when you right-click the Windows Explorer or My Network Places icons. It also removes the Add Network Place option from My Network Places.
- This policy setting does not prevent users from connecting to another computer by typing the name of a shared folder in the Run dialog box.

Appendix G: Internet Connection Wizard and Network Connection Wizard

In Microsoft Windows 2000 Service Pack 3 (SP3) you connect to the Internet with the Internet Connection Wizard. The primary way to make this type of connection is through the Network Connection Wizard in Network and Dial-up Connections.

The content in this appendix includes the following:

- An overview of the Internet Connection and Network Connection wizards
- How to control access to network connection wizards

Overview: Internet Connection Wizard and Network Connection Wizard

Administrators or users with administrative credentials can use the Network Connection Wizard to create any type of network connection including Internet, incoming, dial-up, virtual private network (VPN), and direct connection. In the Network Connection Wizard, if an administrator or user clicks **Dial-up to the Internet** and **Next**, the Internet Connection Wizard appears.

Administrators or users can create a new connection through Settings\Network and Dial-up Connections. When you click **Make New Connection**, the Network Connection Wizard guides you through this process.

When a user clicks on any program for the first time that requires an Internet connection, such as Microsoft Internet Explorer, the Internet Connection Wizard appears. In a highly managed network environment you might want to prevent administrators as well as users from creating new connections.

Controlling the use of network connection wizards

There are various ways you can block access to network connection wizards using Group Policy. You can block administrators and users from making any kind of new connection through the Network Connection Wizard by configuring Group Policy. In User Configuration\Administrative Templates\Network\Network and Dial-up Connections, you configure the policy setting **Prohibit Access to the Network Connection Wizard**. This policy setting does the following:

- It determines whether users can use the Network Connection Wizard, which creates new network connections.
- When this policy setting is enabled, the Make New Connection icon does not appear in the Start menu or in the Network and Dial-up Connections folder. As a result, users cannot start the Network Connection Wizard.
- It does not prevent users from using other programs such as Internet Explorer to bypass this policy setting.

Using Group Policy you can remove Network and Dial-up Connections from the Start menu. In User Configuration\Administrative Templates\Start Menu & Taskbar, you can configure the

following policy setting: **Remove Network & Dial-up Connections from Start Menu**. This policy setting does the following:

- It removes Network and Dial-up Connections from Settings on the Start menu and prevents users from running Network and Dial-up Connections.
- Network and Dial-up Connections still appears in Control Panel and in Windows Explorer, but if users try to start it, a message appears explaining that a policy prevents the action.

You can also disable only the Internet Connection Wizard. In User Configuration\Administrative Templates\Windows Components\Internet Explorer, configure the policy setting: **Disable Internet Connection Wizard**. This policy setting does the following:

- It prevents users from running the Internet Connection Wizard.
- When you enable this policy setting, the Setup button on the Connections tab in the Internet Options dialog box appears dimmed and cannot be selected.
- Users will also be prevented from running the wizard if they click the Connect to the Internet icon on the desktop, or if they click Start, point to Programs, point to Accessories, point to Communications, and then click the Internet Connection Wizard.

This policy setting overlaps with the **Disable the Connections page** policy setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from the interface. Removing the Connections tab from the interface, however, does not prevent users from running the Internet Connection Wizard from the desktop or the Start menu.

For additional information about controlling access to Internet Explorer, see the section in this white paper titled "Internet Explorer 5.01 SP3."

For information about using the Group Policy Object Editor, see Appendix B, "Resources for Learning About Group Policy."

Related Links

This section contains a list of relevant Web sites. Some of the sites are specific sites found in other sections of this white paper. Some are more general sites with links to information about Windows 2000.

Links to product information, support information, TechNet, Microsoft Developer Network, and information in Resource Kits

The following sites provide information about Windows 2000 and other Microsoft products. The list includes sites containing product Help as well as other general sites that provide information about Microsoft operating systems and other Microsoft products:

- Windows 2000:

  www.microsoft.com/windows2000/

- Windows 2000 Help on the Web, including Help for Windows 2000 Professional and for products in the Windows 2000 Server family:

  www.microsoft.com/windows2000/techinfo/proddoc/

- Microsoft Product Support Services:

  support.microsoft.com/

- Microsoft TechNet:

  www.microsoft.com/technet/

- Microsoft Developer Network:

  msdn.microsoft.com/

- Prescriptive Architecture Guides:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/idc/pag/pag.asp

- Windows Deployment and Resource Kits:

  www.microsoft.com/reskit/

- Windows 2000 Server Resource Kit, Supplement 1:

  www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp

- NetMeeting 3 Resource Kit (the NetMeeting section in this white paper provides links to specific chapters in this kit):

  - www.microsoft.com/technet/prodtechnol/netmtng/reskit/netmtg3/cover.asp
  - www.microsoft.com/windows/NetMeeting/Corp/ResKit/

Links to information about security, management, and deployment

The following sites provide information about security, management, and deployment topics:

- Managing mobile code:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/mblcode.asp

- Best practices for enterprise security:
  - www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp
  - www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/default.asp
- Deploying Windows 2000 and deploying Service Pack 3 for Windows 2000:
  - www.microsoft.com/windows2000/techinfo/planning/default.asp
  - www.microsoft.com/windows2000/techinfo/reskit/en-us/w2rkbook/DPG.asp?frame=true
  - www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dgfa_pt6_fhpz.asp
  - www.microsoft.com/windows2000/downloads/servicepacks/sp3/spdeploy.htm
- The **Set Program Access and Defaults** interface (through which you can set the default Web browser, e-mail application, and media player on a desktop), as well as the related programming interface:
  - support.microsoft.com/default.aspx?scid=kb%3ben-us%3b327931
  - msdn.microsoft.com/library/en-us/shellcc/platform/shell/programmersguide/shell_adv/registeringapps.asp
- Windows Script Host:

  www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/sag_WSHtopnode.htm

- Automated installation and deployment:
  - The System Preparation (Sysprep) tool:

    msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kmag00/html/Sysprep.asp

  - Winnt32.exe:

    www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/wqs_qs_03016.htm

  - Unattended setup and Systems Management Server:
    - www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dgcb_ins_adeb.asp
    - www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dgqf_sms_zunm.asp

Links to information about components in Windows 2000 SP3

The following sites provide information about some of the components in Windows 2000 SP3:

- Certificates, certificate status, and certificate revocation:
  - www.microsoft.com/technet/security/prodtech/pubkey/default.asp
  - www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp

- Connection Manager:
  - www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/cmak_ops_03.htm
  - www.microsoft.com/windows2000/en/server/help/default.asp?url=/WINDOWS2000/en/server/help/cmak_ops_12.htm
  - support.microsoft.com/default.aspx?scid=KB;en-us;317593
- HyperTerminal:

  www.hilgraeve.com/support/faq/index.html
- Internet Explorer:
  - www.microsoft.com/windows/ie/
  - www.microsoft.com/windows/ieak/previous/
- Internet Information Services:
  - www.microsoft.com/technet/security/prodtech/windows/iis/default.asp
  - www.microsoft.com/windows2000/server/evaluation/features/web.asp
  - www.microsoft.com/mspress/books/sampchap/4293.asp
  - www.microsoft.com/technet/security/tools/tools/locktool.asp
  - www.microsoft.com/technet/security/tools/tools/urlscan.asp
- Internet Protocol version 6:
  - www.microsoft.com/ipv6
  - www.microsoft.com/windowsserver2003/technologies/ipv6/
  - www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/15_xpip6.asp

    The information in the preceding link can also be obtained by downloading a white paper at the following Web site:

    www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp
- NetMeeting:
  - www.microsoft.com/windows/NetMeeting/
  - www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp
  - support.microsoft.com/default.aspx?scid=KB;en-us;Q158623
  - support.microsoft.com/default.aspx?scid=/support/netmeeting/howto/default.asp

  For additional information about NetMeeting, see "NetMeeting 3 Resource Kit" in "Links to product information, support information, TechNet, Microsoft Developer Network, and information in resource kits" earlier in this section.
- Registration Wizard:

  www.microsoft.com/info/privacy.htm
- Terminal Services and Terminal Services Licensing:
  - www.microsoft.com/windows2000/technologies/terminal/default.asp

  - www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/part4/chapt-16.asp
  - https://activate.microsoft.com/
  - www.microsoft.com/windows2000/en/server/help/default.asp?url=/WINDOWS2000/en/server/help/ts_lice_c_070.htm
  - www.microsoft.com/windows2000/docs/tslicensing.doc
- Windows Media Player:
  - www.microsoft.com/windows/windowsmedia/
  - windowsmedia.com/privacy/privacystatement.asp
  - www.microsoft.com/windows/windowsmedia/privacy/9splayer.asp
  - msdn.microsoft.com/library/default.asp?url=/library/en-us/wmplay/mmp_sdk/windowsmediaplayerskins.asp
  - msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwmt/html/WMPlayer_9_SDK_Intro.asp
- Windows Media Services:
  - www.microsoft.com/windows/windowsmedia/distribute.aspx
  - www.microsoft.com/windows/windowsmedia/serve/deployguides.aspx
  - www.microsoft.com/windows/windowsmedia/serve/firewall.aspx
  - www.microsoft.com/technet/prodtechnol/netshow/plan/wmtbest.asp
  - msdn.microsoft.com/downloads/list/winmedia.asp?frame=true
- Windows Time service:
  - www.microsoft.com/windows2000/techinfo/howitworks/security/wintimeserv.asp
  - www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/operate/wintime.asp
  - support.microsoft.com/default.aspx?scid=kb;en-us;Q223184
- Windows Update:
  - windowsupdate.microsoft.com/
  - corporate.windowsupdate.microsoft.com
  - www.microsoft.com/windows2000/windowsupdate/sus/default.asp

Links to sites maintained by task forces and other organizations

The following sites are maintained by the Internet Engineering Task Force:

- www.ietf.org/html.charters/ngtrans-charter.html
- www.ietf.org/rfc/rfc1510.txt
- www.ietf.org/rfc/rfc2373.txt?number=2373/

- www.ietf.org/rfc/rfc3056.txt?number=3056/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

The following sites are maintained by the International Multimedia Telecommunications Consortium:

- www.imtc.org/
- www.imtc.org/h323.htm

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

The following site is maintained by the International Telecommunication Union:

- www.itu.int/home/index.html

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Links to information about Group Policy

The following sites provide information about topics related to Group Policy:

- Resource Kit Group Policy reference:

  www.microsoft.com/windows2000/techinfo/reskit/en-us/w2rkbook/gp.asp

- Group Policy object settings spreadsheet (this lists policy settings for both Windows 2000 and Windows XP):

  www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

- Implementing Registry-Based Group Policy:

  www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp